

Mit Stellenmarkt

MAGAZIN FÜR PROFESSIONELLE INFORMATIONSTECHNIK

2 Februar 2008 € 5,50 H 10554

Februar 2008

www.ix.de iX Magazin für professionelle Informationstechnik Italien € 6,70 Benelux € 6,70 Schweiz CHF 10,70 Österreich € 6,20

IT-Security:
Change-Management

Tutorial:
C++ mit Boost
Serialisierung und Netzprogrammierung

Neuer Schub durch Android und iPhone:

Programmieren fürs Handy

Mobil ins Internet mit Apple und Google

Softwareentwicklung:
.Net wird dynamisch

Administration:
Nagios 3

Server-Technik:
Amazons Elastic Compute Cloud

Internet-Zugang:
Provider-Wechsel ohne Ärger

Betriebssysteme:
Wie sicher AIX 6.1 ist
Red Hat Enterprise Linux 5.1



Marktübersicht Präsentationstechnik:
Großbildschirme und Projektoren

4 199148 505501 02

Heise

Bill will ...

Mit Aplomb hat Bill Gates auf der Consumer Electronics Show seine letzte große Rede gehalten, in der er als „Keynoter“ Abschied vom lauschenden Fachpublikum nahm. Das amüsierte sich über eingespielte Videos, mit denen Gates seit 20 Jahren seine Keynotes aufzulockern pflegt, und klatschte dankbar Beifall. Die hübsche Inszenierung kam an: „Bill geht“ schrieb die Frankfurter Allgemeine Zeitung und feierte den Visionär Gates mit einem großen Titelbild – um tags danach an gleicher Stelle den Visionär Wilhelm Busch zu preisen. Doch nichts liegt ferner als der „Abschied aus der Welt der Elektronik“, wie die Welt den Ratenrücktritt von Bill Gates kommentierte. Der Microsoft-Gründer bleibt Verwaltungsratsvorsitzender des Konzerns und arbeitet im Monat mindestens 15 Stunden für seine Firma.

Mit 9 Prozent der Aktienanteile im Wert von ca. 30 Milliarden Dollar bleibt Gates größter Einzelaktionär. Entsprechend muten die Bilanzen zum inszenierten Abschied des 53-Jährigen an. Sie lesen sich stellenweise wie Nachrufe, würdigen seine Leistungen im bunten Mischmasch mit der Erwähnung einiger Microsoft-Flops. Bleiben wir einen Moment bei den Leistungen: Zu Gates’ direkten Verdiensten gehört es, das DOS-Betriebssystem gegen harte Konkurrenz auf dem PC durchgesetzt zu haben, mit Geschäftsmethoden, die hart an der Grenze der Legalität lagen.

Ein weiteres Verdienst ist die Entscheidung von Gates, aufbauend auf dem Erfolg von Windows 95 nach der Trennung von IBM mit Windows NT ein System direkt gegen Novells LAN-Monopol zu positionieren und, mit nicht immer feinen Methoden, durchzusetzen. Schließlich muss die Tatsache genannt werden, dass Microsoft den Start des Internet-Booms zwar verpasste, aber Gates in kürzester Zeit eine Neuausrichtung auf das Internet durchsetzte und die Boom-Firma Netscape ausbremste, unter kräftiger Ausnutzung des Marktmonopols von Microsoft. Neben diesem von Gates betriebenen radikalen Geschäftsgebaren hatte Microsoft auch noch Glück mit Aufkäufen wie Multiplan, QDOS oder Powerpoint.

Bei all diesen Manövern waren Visionen weniger wichtig als die richtigen Bandagen und Geschäftsabkommen. In den erwähnten Krisen griff Gates auch zu Methoden, für die Microsoft später Wiedergutmachung leisten musste. Zuletzt zahlte man AOL 750 Millionen Dollar und 7 Jahre kostenlose Browsercode-Nutzung – als der Geschäftsnachfolger von Netscape in der Krise steckte und keine Bedrohung mehr war. Bei allen Manövern aber blieb Microsoft intakt, getrieben von einem Mann, für den „Competition“ immer wichtiger war als „Vision“. Weil selbst der kleinste Wettkampf für Gates eine ernste Sache ist, überzeugt die Inszenierung und vor allem die Begründung seines Rückzugs nicht, er wolle sich voll der gemeinnützigen Stiftungsarbeit widmen. Die Bill & Melinda Gates Foundation, die verdienstvolle große Stiftung, ist ein höchst effizient arbeitender Thinktank und braucht keine Hilfe von Bill. Außerdem ist sie auf Melinda Gates zugeschnitten, die die wichtigsten Keynotes hält.

So stellt sich die Frage, ob nicht ein anderes Motiv hinter dem Rückzug von Gates steckt. Wie wäre es mit der Erklärung, dass Microsoft noch ein bisschen mehr in die Krise schlittern kann, weil Betriebssysteme und Anwendungen immer unwichtiger werden? Wie wäre es mit einem Gates, der nach dem Abschied des amtierenden Chefs Steve Ballmer aus der „Versenkung“ auftaucht und den Konzern wieder auf Kurs bringt? Damit wäre Gates wieder in einem Wettbewerb, sogar in seinem allerliebsten: Er könnte der Welt endlich zeigen, dass er doch der bessere Steve Jobs ist.

DETLEF BORCHERS



Februar 2008

MARKT + TRENDS

TITEL

REVIEW

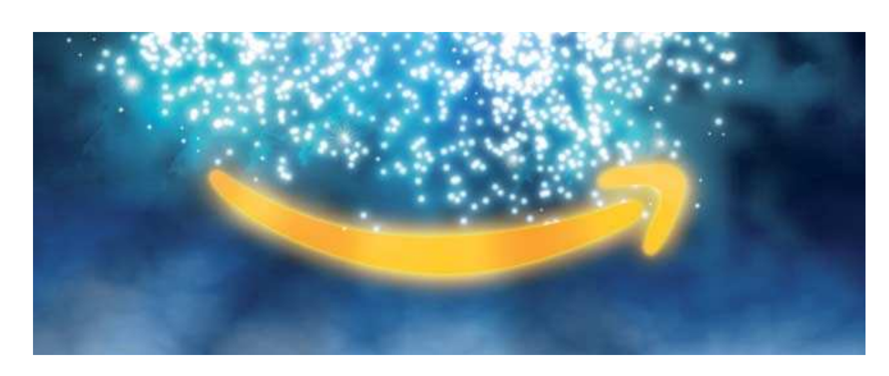
REPORT



Systemüberwachung à la carte: Nagios 3

Wahrscheinlich ist gerade die Tatsache, dass Nagios nicht alles selbst erledigen will, sondern geschickt Drittwerkzeuge als Plug-ins einbindet, ein Grund für seinen Erfolg. Und mit Version 3 sind noch einmal etliche Verbesserungen dazugekommen – vor allem „unter der Haube“.

Seite 54



Rechenzeit kaufen bei Amazon

Durch den Betrieb seines Onlinebuchversands dürfte bei Amazon viel Know-how in Sachen Serverbetrieb aufgelaufen sein. Dass man dort jetzt auch Rechenzeit kaufen kann, ist darum naheliegend, aber bislang wenig bekannt. *iX* hat es einige Monate lang ausprobiert.

Seite 64



Sichere Software-installation

Wer jedes Software-Upate sofort einspielt, zeigt zwar viel guten Willen, erreicht aber nicht unbedingt den gewünschten Effekt. Denn oft werden dadurch eben behobene Sicherheitslücken wieder geöffnet, ganz zu schweigen von unerwarteten Seiteneffekten. Change-Management soll’s richten.

Seite 112



Programmieren fürs Handy

Mit Apples iPhone und Googles Betriebssystem Android ist neuer Schwung in die Welt der mobilen Applikationen gekommen. Da lohnt sich auch für bislang Handy-kritische Softwarehäuser ein längerer Blick auf die neuen Benutzeroberflächen und APIs. Details zum Mac OS X fürs Mobile, dem Betriebssystem des Suchmaschinengiganten und den aufkommenden Sicherheitsproblemen.

Seiten 34, 38 und 42



Großbildschirme und Projektoren

Statt des Hausmeisters sind heute die IT-Abteilungen zuständig für Anschaffung und Betrieb professioneller Projektionstechnik. Grund genug, sich einen Überblick über die aktuellen Produkte zu verschaffen und Einblick in den Stand der Technik zu nehmen.

Seiten 72 und 118



WISSEN

PRAXIS

MEDIEN

RUBRIKEN

Cool, das iPhone.

(Mobile Computing: Apples iPhone als Geschäftstelefon; *iX* 1/08; S. 68)

Zuerst war ich begeistert von meinem neuen iPhone – elegant, schick, cool, tolle Funktionen!

Nach der ersten Euphorie kam ich etwas ins Zögern: Hhhmmm, Batterie ist ziemlich schnell alle – naja, hab ja viel damit herumgespielt, und allen Freunden und Geschäftskollegen stolz mein Super-Telefon vorgeführt.

Dabei hab ich immer kontrolliert, welche Seiten angesurft wurden – wollte mich nicht blamieren. Flash oder Java geht nämlich nicht.

Auch die Tatsache, dass alle Fotos, die ich damit gemacht habe, in einem festen Ordner landen und dort mittlerweile 200 Bilder von der Computermesse über den Weihnachtsspaziergang und dem gemütlichen Abend bei Wein und Pasta bunt gemischt werden, hat mich nicht sonderlich gestört. Die kann ich sicher beim Übertragen auf meinen PC separieren – ist ja cool, das iPhone!

MMS? Nein, das iPhone kann ja Bilder per Mail versenden. Also MMS geht auch nicht, auch nicht empfangen – ist ja cool, das iPhone!

Allerdings war ich schon nicht mehr so vergnügt, als ich meine E-Mails einzeln löschen musste. Ich hatte sicher 150 E-Mails über die Ferien bekommen. Jede einzelne muss manuell gelöscht werden. Die Funktion „alle löschen“, oder „markieren“ fehlt. So hab ich mit Fingerkrämpfen die Mails in den Papierkorb verschoben – oops, diese Mail nicht in den Papierkorb, da ist sie, aber zurück in den Posteingang? – Geht nicht … ist ja cool, das iPhone.

Langsam machte ich mir Sorgen. iTunes hatte ich ja auf meinem PC installieren müssen, um das iPhone zum Laufen zu bringen. Ein Musikprogramm zur Verwaltung des Telefons? Meine Kreditkarte wollte Apple auch haben? Klar, MP3-Klingeltöne gehen ja nicht.

Jetzt ist es kaputt, die Lautstärke-Taste klemmt, Anruf bei T-Mobile – klar, einschicken, Dauer 1 bis 2 Wochen. Ersatz-iPhone – klar, nein. „Bitte sichern Sie vorher Ihre Daten“ – klar, mach ich. T-Mobile gab mir noch netterweise die Telefonnummer des Apple-Callcenters. Selber hatten die keine Ahnung, wie das geht.

Ich befasse mich kurz mit iTunes – der mitgelieferten Software für meinen PC. Was haben „Party-Jukebox“, „Fernsehsendungen“ und „iTunes Store“ mit einer Datensicherung zu tun? Ich rufe beim Apple-Callcenter an, um mit professioneller Hilfe die Daten zu sichern. Kurz: Ein Desaster. Nach genauer schrittweiser Anweisung durch den Callcenter-Profi wurden zuerst alle meine Kontakte komplett vom iPhone gelöscht (auch wiederholt im Nachhinein nachvollziebar, das dumme iTunes synchronisiert erst einmal das leere Windows-Adressbuch auf das iPhone!). Sie sind unwiederbringlich verloren. Dann hat er schnell aufgelegt und war nicht wiederzufinden.

Sein Kollege unterbreitete mir dann, dass ich die Kontakte, Termine, E-Mails und Bilder nicht sichern könnte, SMS sowieso nicht – nur synchronisieren, aber nur ab Office 2003 und Photoshop, und zuerst nur in Richtung iPhone, damit gehen beim ersten Synchronisieren alle iPhone-Adressen verloren! Wie bitte?

Für die Bilder hatte er doch noch eine Idee: Ich könnte sie mir ja selber mailen – einzeln, versteht sich, man kann ja die Bilder nicht markieren – 200 Bilder!

iPhone zu verkaufen, voller Kinderkrankheiten, leicht kaputt – ist nicht mehr cool, das iPhone …

DIETRICH V. WITZLEBEN, MÜNCHEN

Flugmeilen einsparen

(IT und Klimaschutz: Strategien gegen die Energieverschwendung; *iX* 1/08; S. 112)

Betrachtet man die Energiebilanz, ist sicherlich auch Second Life nicht die beste aller Welten. Es jedoch nur unter dem Aspekt „schlecht ausgenutzte Serverkapazitäten“ zu beurteilen, greift meines Erachtens viel zu kurz!

DER DIREKTE DRAHT ZU iX

Direktwahl zur Redaktion: 05 11/53 52-387

Bitte entnehmen Sie Durchwahlnummern und E-Mail-Adressen dem Impressum.

Redaktion iX
Postfach 61 04 07
30604 Hannover

Fax: 05 11/53 52-361
E-Mail: <user>@ix.de
Web: www.ix.de

Sämtliche in iX seit 1990 veröffentlichten Listings sind über den iX-FTP-Server erhältlich: ftp.heise.de/pub/ix/

Dass durch die Möglichkeiten der Online-Collaboration große Unternehmen mit dem Gedanken warm werden (;-)), Meetings und Fachkonferenzen in virtuellen Welten abzuhalten und dadurch in Zukunft zahllose Flugmeilen eingespart werden können, entgeht der Autorin.

Wem das nicht reicht, der kann seinen Avatar oder seinen Sim zum Beispiel beim Realeaf-Projekt (www.forcesunrise.com/de/realeaf/) CO_2-neutral kaufen, indem er ein Klimaschutzprojekt mit Linden-Dollar unterstützt. Eine bessere Lösung fällt den Branchengrößen ja schließlich auch nicht ein.

TORRID LUNA,
VIA E-MAIL

Blacklists und dynamische IP-Adressen

(Internet: Echtzeit-DNS-Blacklist als Waffe gegen Spam; *iX* 12/07, S. 112)

Vielen Dank für Ihren informativen Artikel über Echtzeit-Blacklists. Das erneute Einschalten Ihrer DNSBL hat die Anzahl meiner pro Woche eintreffenden Mails von ca. 1000 auf ca. 700 reduziert (was natürlich immer noch eine lächerlich hohe Zahl ist, wenn man bedenkt, dass ich pro Woche 30 bis 50 Mails bekomme, welche kein Spam sind).

Dennoch möchte ich Sie auf eine Ärgerlichkeit im Zusammenhang mit Blacklists aufmerksam machen, welche mir seit circa einem Monat Kopfzerbrechen bereitet: Sendet man eine E-Mail von einer dynamischen IP-Adresse aus über einen SMTP-Server, so schreibt dieser einen Received-Header in den Header der E-Mail. Dieser wiederum wird häufig genug von einer Spamassassin-Instanz bzw. einem anderen Spamfilter gelesen und ausgewertet, nicht selten, indem die Einträge des Headers auf Treffer in verschiedenen Blacklists (und ebenfalls in Dial-Up-Lists) untersucht werden. Die o. g. Ärgerlichkeit ist die, dass viele E-Mails, die von meinem Server ausgehen, nämlich solche, welche von einem lokalen Mailclient per SMTP an meinen Server übertragen wurden, in Spamfiltern landen oder zumindest schon von vornherein einen recht beachtlichen „Spamscore“ haben.

Eine Anfrage bei den Entwicklern von Spamassassin brachte mir nur die Antwort, dass die meisten E-Mail-Nutzer keine lokalen Mailclients benutzen, sondern einen Webmail-Client oder eine feste IP haben, und dass dies Pech sei. Für mich keine zufriedenstellende Antwort.

Haben Sie vielleicht eine Lösung für dieses Problem, außer auf Webmail umzusteigen?

FLORIAN KRIENER,
LEIPZIG

Sie beleuchten einen wichtigen Aspekt beim Einsatz von Blacklists. Die geschilderten Probleme sind jedoch nicht auf den Spamassassin an sich zurückzuführen, sondern auf die Auswahl der richtigen Blacklists.

Im Prinzip spricht nichts dagegen, den gesamten Header auf IP-Adressen hin abzusuchen und diese auf Blacklist-Eintragungen hin zu prüfen. Jedoch muss dann sichergestellt sein, dass die abgefragten Blacklists ausschließlich Adressen enthalten, die tatsächlich in letzter Zeit als Spam-Quellen in Erscheinung getreten sind. Dazu gehören etwa Spamcop oder auch die im Artikel beschriebene iX-Blacklist.

Ungeeignet sind in diesem Fall Blacklists, die IP-Adressen allein deswegen enthalten, weil sie von Providern als dynamisch vergebbar gekennzeichnet wurden. Damit würde man nicht nur Mails von Webmail-Anwendern, sondern auch vieler Smarthosts als verdächtig einordnen, nur weil sie über einen solchen Zugang verfügen. Die meisten Webmail-Server und Smarthosts dokumentieren nämlich die tatsächliche IP-Adresse des Absenders.

Dennoch haben Listen dynamisch zugeteilter IP-Adressen ihren Sinn. Wer die Policy umsetzt, keine Mails direkt von solchen Adressen anzunehmen, darf dann aber auch nur diejenige des unmittelbaren SMTP-Clients heranziehen und nicht alle, die sich im Header finden lassen. (Bert Ungerer)

Ergänzungen und Berichtigungen

(Computerforensik: Massendaten sichern mit dem TreCorder; *iX* 1/08; S. 78)

In der Messtabelle zum TreCorder sind zwei Einträge der zweiten Überschriftenzeile nach rechts verrutscht: „(Binärpräfixe)“ und „in GByte“ gehören zur Spalte „Kapazität“.

24C3: Spontandemo gegen Überwachung und Vorratsdatenspeicherung

Volldampf Richtung 1984

Christoph Puppe

Die Sorge um den Verlust von Bürgerrechten und des letzten Rests an Privatsphäre trieb rund 1000 Hacker auf den Berliner Alexanderplatz. Dort demonstrierten die sich traditionell zum Jahresende versammelnden Teilnehmer des Chaos Communication Congress gegen die nun endgültig abgesegnete Vorratsdatenspeicherung.

Mit einer spontaner Demonstration gegen Vorratsdatenspeicherung mit dem Slogan „Guten Rutsch ins Jahr 1984" setzten die Teilnehmer des traditionell zum Jahresende stattfindenden Chaos Communication Congress einen starken Akzent gegen den Abbau von Privatsphäre und die Einschränkung des Rechts auf informationelle Selbstbestimmung.

Den über 4000 Besuchern bot sich im schon bekannten Berliner Congress Center eine abwechslungsreiche Zeit mit den fast sämtlich auf Englisch gehaltenen Vorträgen sowie stolzen 25 wissensvermittelnden Workshops. Die 100 Vorträge verteilten sich thematisch auf die Kategorien „Society", „Culture" und „Hacking". Der neu hinzugekommene Track „Making" steht in der Tradition des Magazins „Make" aus dem O'Reilly-Verlag und widmet sich dem Selbstbasteln von Dingen, grob gesagt.

Kampfstricker am Werk

Themen dieses Tracks waren unter anderem die freie Geodatenbank OpenStreetMap, wie man einen Roboter-Aufstand überlebt, selbstgebaute Drohnen und das in Hackerkreisen wundersamerweise so beliebte Stricken – Letzteres mit dem vielversprechenden Titel „The history of guerilla knitting". Martin Müller und Antoine Drouin boten mit ihrem Vortrag „Paparazzi – The Free Autopilot" einen Einblick in eine Open-Source-Entwicklung eines autonom fliegenden Modellflugzeugs. Der beeindruckende Film der im Flugzeug angebrachten Kamera zusammen mit den Details des Projektverlaufs und der GPS-basierten Steuerung begeisterte die Zuschauer. Der Track „Science" bot thematisch von einer Analyse ansteckender Krankheiten in World of Warcraft über die Art und Weise der DNA-Programmierung bis hin zu Verschwörungstheorien viel Überraschendes.

Mit Spannung erwarteten die Zuschauer den eher „klassischen" Hacking-Vortrag von FX von Phenoelit zur Sicherheit von Barcodes. Nach einer Einführung zu Geschichte und Einsatzzweck des Barcodes – etwa für IDs, Tags, Datentransport oder „GGU" (ganz grober Unfug) – erläuterte er, was man mit manipulierten Scannern oder Barcodes anstellen kann: einen Badge, der als Zahlungsmittel an der Bar gilt, mehrfach kopieren, ein temporär gültiges Parkticket in einer Dresdener Hotelgarage in ein unbegrenzt gültiges für kostenloses Parken umwandeln oder auch Schummeleien mit Pfandsystemen. Summa summarum weisen alle gängigen Barcode-Systeme gravierende Sicherheitsmängel auf.

Luke Jennings führte einen von ihm selbst entwickelten Angriff gegen unter Windows gespeicherte Zugangs-Token vor. Mit seiner Software lassen sich die Access-Token der Domänen-Administratoren dazu benutzen, sämtliche Aktionen in einer Windows-Domain auszuführen, die sonst dieser Gruppe vorbehalten sind. Ein Domänen-Admin muss sich nur einmal seit dem letzten Booten in den vom Angreifer übernommenen PC eingeloggt haben, damit dies möglich wird. Jennings hat das notwendige Werkzeug auf Sourceforge veröffentlicht.

Unsichere Steuerungsprozesse

Der jüngste Vortragende war auch gleichzeitig der am weitesten gereiste, der 17-Jährige kuza55 war aus Australien nach Berlin gekommen, um einen Vortrag über Tricks beim Hacken von Webapplikationen zu halten. Weitere Beiträge behandelten Unsicherheiten bei Oracle, das Sniffen von 10-Gigabit-Ethernet, zielgerichtete Angriffe mit Malware, den Storm Worm, das Cracken von Sonys Playstation Portable sowie das Hacken von SCADA. SCADA ist kein Betriebssystem, das keiner kennt, sondern die Abkürzung für „Supervisory Control and Data Acquisition", sprich die Steuerung von Prozessen in der Industrie, von Fließbändern, über Öl-Förderungsanlagen bis hin zu Kraftwerken. Mayhem und Raoul „Nobody" Chiesa zeigten erfolgreiche Angriffe gegen solche Anlagen und konnten überzeugend darstellen, dass sie ziemlich einfach durchzuführen sind.

Der zur Tradition gehörende Vortrag „Security Nightmares" von Ron und Frank Rieger über die wichtigsten Sicherheitsprobleme und „worüber wir nächstes Jahr lachen werden" bot am letzten Tag einen gewohnt heiteren Abschluss dieses Tracks. 2007 brachte beispielsweise den Superwurm in Form des kombinierten Schadprogramms „Storm Worm" und weitere Malware mit auffälligen Schadroutinen. Fürs kommende Jahr rechnen die Hacker mit einer Zunahme von Schadcode für iPhone & Co. sowie einem verstärkten Handel mit Exploits.

Im Track „Society" war das Unwort des Jahres 2007 „Bundestrojaner", auch Thema eines Vortrags von Andreas Bogk, Constanze Kurz und Felix von Leitner. Unter der Überschrift „Die Wahrheit haben wir auch nicht, aber gute Mythen" boten sie einen Überblick und reichlich Details zu den technischen und gesellschaftlichen Diskussionen. Lesenswert dazu ist auch das Buch „1984.exe" von Constanze Kurz. Die zahlreichen weiteren Überwachungs- und Datensammelprojekte der Bundesregierung, aber auch der EU – Stichworte Vorrats- und Flugdatenspeicherung, RFID, Copyrightverschärfung – trugen dazu bei, dass es diesem Track nicht an Vorträgen mangelte.

Der CCC wäre jedoch nicht er selbst, wenn nicht auch Gegenmaßnahmen zur Sprache kämen – etwa in den Vorträgen „23 Wege, für Deine Rechte zu kämpfen" und „Distributed campaigns for promoting and defending freedom in digital societies". Und den Erfolg seines gesellschaftspolitischen Engagements hat der Club im vergangenen Jahr mit seiner Kampagne gegen die umstrittenen, weil unsicheren Wahlcomputer hinreichend bewiesen. (ur)

Onlinequellen

Kongress-Homepage	events.ccc.de/congress/2007/Main_Page
Mitschnitte der 24C3-Beiträge	events.ccc.de/congress/2007/Conference_Recordings
Magazin „Make	makezine.com/magazine
Freie Geodatenbank:	www.openstreetmap.de
Phenoelit:	www.phenoelit-us.org
Tool zur Manipulation von Windows-Zugangs-Token:	sourceforge.net/projects/incognito
Constanze Kurz, 1984.exe	www.transcript-verlag.de/ts766/ts766.htm

Informationstechnik ist Chefsache

Geschliffen

Barbara Lange

Informations- und Kommunkationstechnik haben sich in den letzten 10 Jahren zur Chefsache bei Medien, Wirtschaft und Politik entwickelt. Wie der Standort Deutschland hier international ganz vorne mitspielen kann, diskutierten führende Vertreter aus Wirtschaft und Politik beim zweiten IT-Gipfel der Bundesregierung.

Rund 400 Teilnehmer aus Behörden, Unternehmen und wissenschaftlichen Instituten trafen sich am 10. Dezember im Convention Center auf dem Hannoverschen Messegelände, darunter führende Bundes- und Landespolitiker: Vertreten waren Bundeskanzlerin Angela Merkel und die Bundesminister Wolfgang Schäuble, Michael Glos und Brigitte Zypries sowie der niedersächsische Ministerpräsident Christian Wulff und Wirtschaftsminister Walter Hirche.

Wirklich Neues im Vergleich zum ersten IT-Gipfel im Jahre 2006 war schwer auszumachen, und vieles ist aus der Tagespresse bekannt, zum Beispiel die Ernennung eines Bundes-CIO ab Januar 2008, der die Modernisierung der IT in Bund, Ländern und Kommunen koordinieren soll. Die Schließung von „Breitbandlücken“ und der weitere Ausbau von Netzen und Diensten gelten als Voraussetzung dafür, dass Deutschland seine internationale Position ausbauen kann. Sogenannte Leuchtturmprojekte wie die Suchmaschine Theseus, das Internet der Dinge oder die einheitliche Behördennummer 115 will man weiter fördern. Neu hinzugefügt wurde das Thema grüne IT.

Auch wenn die Reden und Erklärungen der Anwesenden oft schwindelerregend allgemein blieben, gibt es doch Entwicklungen bei einzelnen Leuchtturmprojekten: So hat die Bundesnetzagentur im Dezember dem Bundesinnenministerium die Nummer 115 zugeteilt. Pilotprojekte sollen ab der zweiten Hälfte 2008 in den Modellregionen starten. Für die Bedürfnisse des Mittelstands will man ein Informationsportal einrichten, das die vorhandenen dezentralen Angebote bündelt.

Erst hiesige Fachkräfte fördern

Geteilter Meinung waren Wirtschaft und Politik bei der Einwanderung von Fachkräften aus Nicht-EU-Ländern: So will die Bundesregierung zunächst heimische Fachkräfte qualifizieren, „bevor wir uns im zweiten Schritt ausländischen Fachkräften zuwenden“, sagte Bundeskanzlerin Merkel. Auch soll in den Universitäten mehr gefördert und weniger ausgesiebt werden.

Am späten Vormittag traf man sich in vier als „presseoffen“ und „hochrangig“ gekennzeichneten Diskussionsrunden. In Gruppe 4 ging es um IT-Sicherheit und Vertrauen. Große Hoffnungen setzten die Teilnehmer – unter ihnen Bundesinnenminister Schäuble und Bundesdatenschützer Peter Schaar – in den elektronischen



Darf auf keiner IT-Konferenz fehlen: Bundesinnenminister und Überwachungsfan Wolfgang Schäuble.

Personalausweis, der durch seine Vorbereitung für die digitale Signatur sicheren E-Commerce und E-Government ermöglichen soll.

Ob der Fingerabdruck dort wirklich gespeichert werden muss, war der einzige strittige Punkt der trauten Versammlung. Schaar, in diesem Jahr im Vergleich zum 1. IT-Gipfel 2006 offiziell eingeladen, hielt dies für überflüssig, da die Identität und Fälschungssicherheit durch das biometrische Gesichtsbild ausreichend gewährleistet sei. Er betonte auch die Verantwortung der Anbieter beim Umgang mit ihren Kundendaten.

Warteschleifen kostenlos

Vertrauen in die digitale Wirtschaft können Nutzer nur aufbauen, wenn sie einen kompetenten Service erleben – und nicht stundenlang in kostenpflichtigen Warteschlangen festhängen. Den „Leitfaden für eine verbraucherfreundliche Kundenbetreuung“ präsentierte Ursula Heinen, Parlamentarische Staatssekretärin beim Bundesminister für Ernährung, Landwirtschaft und Verbraucherschutz. Warteschleifen müssen für die Nutzer kostenfrei sein, heißt es in diesem von diversen Bundesministerien gemeinsam mit Unternehmen wie Arcor und der Deutschen Telekom erarbeiteten Papier, das sich besonders an Telekommunikations- und Internet-Anbieter sowie Unternehmen richtet, die externe Call-Center mit dem Kundenservice beauftragen wollen.

Dass Bund und Länder bei der Nutzung von IT-Standards kooperieren müssen, will Bundesjustizministerin Zypries im Grundgesetz festschreiben. Die Kooperation unterschiedlicher Behörden in Bund und Ländern ist zum Beispiel für die Umsetzung der Behördennummmer 115 oder der EU-Dienstleistungsrichtlinie erforderlich.

Unter www.it-gipfel.de ist die Veranstaltung gut dokumentiert. Wer gerne Broschüren und Erklärungen liest, kommt dort auf seine Kosten. Den dritten IT-Gipfel will die Bundesregierung 2008 in Darmstadt ausrichten. (ur)

iX-Veranstaltungen

Neu aufgenommen in die *iX*-Workshop-Reihe wurde ein Thema, das in der professionellen Programmierung zunehmend an Bedeutung gewinnt: **Produktlinienentwicklung**, eine quasi industrielle Methode der langfristigen Wiederverwertung. Die Referenten, Klaus Schmid und Holger Eichelberger von der Universität Hildesheim, sind bekannte Experten auf diesem Gebiet. Die eintägigen Workshops finden am 5. und 13. März in Frankfurt/M. respektive München statt. Wer bis Ende Januar bucht, spart gut 13 % der Teilnehmergebühren.

Beim Schreiben dieser Zeilen war der **Kerberos-Workshop** in München bereits ausgebucht, in Düsseldorf waren noch vier Plätze frei, mit ein bisschen Glück ergattern Sie ja vielleicht noch freie Plätze in Zürich.

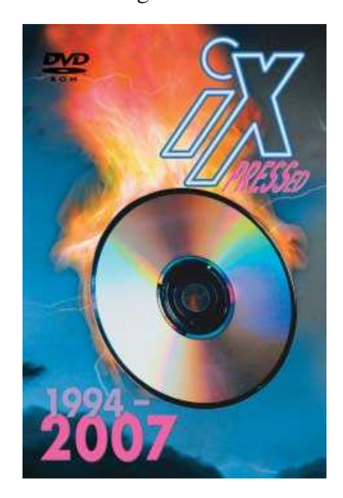
Die kurzfristig angesetzten Workshops zum **Anforderungsmanagement** und die **Teamconf 2008** wurden an dieser Stelle ja schon erwähnt, die letztgenannte Konferenz dreht sich um Microsoft Visual Studio Team System (München, 22. – 24. April). Details wie immer auf der Konferenz-Website www.ix.konferenz.de.

www.ix-konferenz.de

iX-Archiv-DVD 1994–2007 erschienen

Ab sofort lieferbar ist die *iX*-PRESSed-DVD mit dem redaktionellen Inhalt der Jahrgänge 1994 bis 2007, wie immer im HTML-Format. Windows-Anwender kommen zudem in den Genuss des eMedia Navigator, dessen fehlertolerante Suchfunktionen auch unter Linux und Mac OS verfügbar sind. Bis zum 31. Januar gilt ein Einführungspreis von 59 €; der reguläre Preis beträgt 69 €. Erhältlich ist die DVD bei eMedia.

Wer sich nur für die Artikel des Jahrgangs 2007 interessiert, kann auf die CD-ROM iXPRESSed 2007 zurückgreifen (24,50 €). Auch die Jahrgänge 1988 bis 1993 liegen in digitaler Form vor. Hier ist das Dokumentformat PDF, eine Volltextsuche über alle Artikel ist möglich. Preis: 15 €.



Blu-ray gewinnt Formatrennen

Anfang November 2007 sah Sony-Chef Howard Stringer das Rennen zwischen dem hauseigenen Blu-ray und HD DVD noch als unentschieden an. Zwar waren in den ersten drei Quartalen doppelt so viele Blu-ray-Discs wie HD DVDs über die Ladentheken gegangen, doch mit Paramount und Dreamworks hatten sich zwei große Hollywood-Studios zumindest für die nächsten 18 Monate zur HD DVD bekannt, angeblich motiviert durch 150 Millionen US-Dollar von Toshiba.

Doch Anfang Januar, zur Consumer Electronics Show in Las Vegas, wendete sich das Blatt: Warner Bros. kündigte an, der HD DVD in Kürze die Unterstützung zu entziehen und stattdessen von den HD-Formaten nur noch Blu-ray zu unterstützen. Die HD DVD Promotion Group sagte daraufhin eine Pressekonferenz im Rahmen der CES ab, Toshiba zeigte sich überrascht und äußerte Unverständnis. Dass die Warner-Entscheidung durch finanzielle Zuwendungen seitens Sony motiviert sei, dementierte Kevin Tsujihara, Präsident von Warner Home Entertainment. Das Studio habe einzig und allein das Wachstum des HD-Video-Marktes im Auge.

Das Rennen zwischen den beiden HD-Formaten, das sich als Wachstumsbremse beim Umstieg auf neue Geräte herausgestellt hatte, gilt damit als entschieden. Obendrein will man auf eine der bei den Endkunden wohl unbeliebtesten Maßnahmen der DVD-Welt bei Blu-ray verzichten: Ein Warner-Sprecher betonte gegenüber heise online, dass man keine Regionalcodes für die kommenden Scheiben einführen wolle.

Mehrere Updates für Debian

Beim Debian-Projekt standen zum Jahreswechsel zwei große Erneuerungsrunden an. So gaben die Entwickler das inzwischen siebte Update für die Version 3.1 („Sarge“) sowie die zweite Aktualisierung des aktuellen Stable-Zweiges („Etch“) frei. Wer sein System regelmäßig mit Updates von security.debian.org versorgt hat, muss nur wenige Pakete einspielen. Da bei beiden Versionen auch der Installer überarbeitet wurde, funktionieren die bisherigen Netboot- und Disketten-Images nicht mehr. Angepasste Versionen – auch der CD- und DVD-ISO-Images – finden sich auf den Servern des Projekts oder einem der zahlreichen Spiegel (www.debian.org/mirror/list).

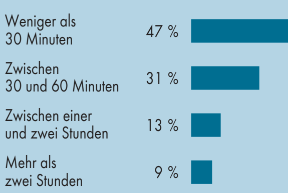
Erwünschte E-Mails unter einem Prozent

Nach übereinstimmenden Angaben mehrerer Anti-Spam-Dienstleister ging der Anteil erwünschter E-Mails an der Gesamtzahl umlaufender Nachrichten im Laufe des vergangenen Jahres erneut deutlich zurück, zum Teil um den Faktor zehn. Waren Anfang 2007 immerhin noch rund 10 Prozent aller E-Mails kein Spam, ließen sich zum Ende des Jahres erwünschte E-Mails an einigen Tagen nur noch in Bruchteilen eines Prozents ausdrücken: Am dritten Adventswochenende etwa zählte Retarus erstmals einen Spam-Anteil von über 99 Prozent. Mit der wachsenden Stückzahl von Spam-Mails sank jedoch deren Größe, wie Eleven aus Berlin feststellte, sodass sich das übertragene Datenvolumen im Laufe des Jahres wenig änderte. Während die Spammer Anfang 2007 mit großen Bildern und sogar zeitweise mit MP3-Dateien experimentierten, setzen sie derzeit vornehmlich auf kurze Texte mit schlichten URLs.

iX-Umfrage: E-Mail-Nutzungsdauer

In Online- und Print-Medien immer wieder kolportierte Meldungen zu überbordender E-Mail-Nutzung kann zumindest die aktuelle *iX*-Umfrage zum Thema nicht belegen. Rund drei Viertel der Teilnehmer verbringt weniger als eine Stunde pro Tag mit dem Bearbeiten elektronischer Post, fast die Hälfte sogar weniger als 30 Minuten. Zu den „Heavy Users“, die täglich länger als zwei Stunden mit ihrer Mail verbringen, rechnen sich nur 8 Prozent. Die Details zur Frage „Wie viel Zeit verbringen Sie im Durchschnitt pro (Werk)Tag mit dem Bearbeiten von E-Mail?“:





Die nächste Umfrage, die mit Erscheinen dieses Heftes startet, dreht sich um eventuelle Konsequenzen aus den neuen Vorschriften zur Vorratsdatenspeicherung von Kommunikationsverbindungen.

Wissensportale: Der Spiegel und Googles Knol

Wie Udi Manber, der Vice President Engineering, im offiziellen Google-Blog mitteilte (http://googleblog.blogspot.com/2007/12/encouraging-people-to-contribute.html), will der Suchmaschinenbetreiber unter dem Codenamen „Knol“ eine eigene Wissensbasis aufbauen, die in direkter Konkurrenz zu Wikipedia stehen dürfte. Wie bei Wikipedia sollen Fachleute Artikel schreiben, allerdings will Google die Position der Autoren hervorheben. Ein Beispielartikel über Schlafkrankheit dient Manber als Hinweis darauf, wie Google sich das Ganze vorstellt.

Zunächst soll das Prozedere auf Einladungsbasis voranschreiten, später soll es wie Wikipedia frei zugänglich sein, weswegen Google jetzt schon auf mögliche Qualitätsunterschiede hinweist. Unter einem Knol, abgeleitet von knowledge, versteht Google sowohl das Gesamtprojekt als auch den einzelnen Artikel als Wissenseinheit – und will das Projekt selbst sowie Tools dafür auf Websites vorhalten.

Nach der New York Times will das deutsche Nachrichtenmagazin „Der Spiegel“ seine Inhalte abgesehen vom jeweils aktuellen Heft kostenfrei online veröffentlichen. Darüber hinaus wollen die Hamburger gemeinsam mit Bertelsmann ein Wissensportal erstellen, das außer den Spiegel-Artikeln seit 1947 Lexika und Wörterbücher sowie die Wikipedia-Inhalte enthalten soll. wissen.spiegel.de, hinter dem ein Tomcat-Server steckt, erfordert derzeit noch eine Authentifizierung.

Wikimedia will durchstarten

Nach dem Umzug von Florida nach San Francisco will die Wikimedia Foundation einige Wikipedia-Vorhaben voranbringen. Im Mai soll es mit den schon länger angekündigten gesicherten Artikeln losgehen. Außerdem plant die Foundation gemeinsames Editieren von Videos in ihren Projekten. Und mit der Mainzer Pediapress (pediapress.com) sollen die Wiki-Einträge sich künftig in PDF sowie später ins OpenDocument-Format exportieren lassen.

Zwar hat die Wikimedia Foundation kürzlich durch eine Spendenkampagne über zwei Millionen Dollar erhalten, das Budget fürs laufende Geschäftsjahr beläuft sich jedoch auf 4,6 Millionen. Die neue Geschäftsführerin Sue Gardner soll unter anderem Großspender vom Projekt überzeugen.



Ruby on Rails: Mitte Dezember 2007 haben die Entwickler von Ruby on Rails die lang erwartete Version 2.0 ihres Web-Frameworks freigegeben. Wie angekündigt, ist die wichtige Neuerung, dass RoR jetzt REST statt SOAP als Standard für Webservices nutzt (www.rubyonrails.org).

RSS: Extralabs Software bietet seinen Feed Editor für die Erzeugung von RSS Feeds zum Preis von 35,96 US-$ in einer Einzellizenz und als Sitelizenz für 1999,95 US-$ an (www.extralabs.net). Das Werkzeug eignet sich laut Hersteller auch für Nicht-RSS-Gurus, kennt unterschiedliche RSS-Formate und erlaubt den Import von CSV- und HTML-Dateien.

Webentwicklung: Die Javascript-fokussierte (wie es beim Hersteller heißt) Webentwicklungsumgebung Studio hat die in San Mateo, Kalifornien, ansässige Aptana jetzt in Version 1.0 fertiggestellt. In der Community Edition ist Aptanas Studio kostenlos, die Professional Edition beläuft sich auf 199 US-$ (der Einführungspreis lag im Januar bei 99 $). Eine Trial-Version ist verfügbar und mutiert nach dem Ausprobieren zur Community Edition (www.aptana.com).

Mehr Webserver: Bei den monatlichen Webserver-Befragungen der britischen Netcraft (www.netcraft.com) hat sich übers Jahr 2007 ein Plus an 5,4 Millionen Webservern ergeben, insgesamt über 155 Millionen Sites antworten nun. Trotz leichten absoluten Zuwachses im Dezember hat der Apache weiter an Dominanz gegenüber Microsofts IIS verloren, führt aber weiterhin (Dezember: 49,57 %). In absoluten Zahlen hat die Zahl der IIS-Sites deutlicher zugenommen (35,76 %).

Blogging: Movable Type, früherer Platzhirsch unter den Blogging-Systemen, war in der Vergangenheit in einer kostenlosen und mehreren kommerziellen Versionen verfügbar. Jetzt hat Hersteller Six Apart (www.sixapart.com), wie schon im Sommer 2007 abgekündigt, eine Open-Source-Fassung der Version 4 freigegeben (www.movabletype.org).

Mehr Internet: Nach einer Umfrage der European Interactive Advertising Association (EIAA, www.eiaa.net) in zehn west- und südeuropäischen Ländern steigt der Internetkonsum weiterhin an. 29 % der Nutzer (= 48 Mio. Menschen) seien mehr als 16 Stunden pro Woche online. Über 80 % können subjektiv nicht auf das Medium verzichten.

XML: Die rumänische Syncro Soft hat Version 9.1 ihres für Windows, Mac OS X und Linux verfügbaren XML-Editors Oxygen fertig. Er kann sowohl mit Schemata als auch mit DTDs, Relax NG und Schematron umgehen und unterstützt außer XPath und XSLT XQuery-Debugging. Neu ist eine erleichterte Eingabe von Attributen und die Konvertierung von DITA-Dokumenten in HTML oder PDF (www.oxygenxml.com).

Suchen: Wikia

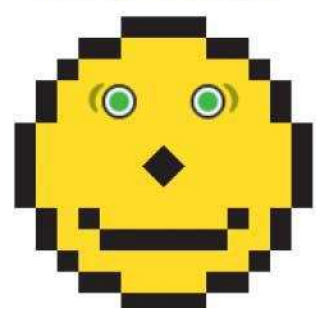
Vor fast einem Jahr schon im Gespräch, hat Wikipedia-Mitgründer Jimmy Wales am 7. Januar 2008 sein Suchmaschinenprojekt Wikia Search in einer ersten Alphaversion online gestartet (search.wikia.com/wiki/Search_Wikia).

Das Projekt soll eine Open-Source-Suchtechnik beinhalten, die beispielsweise den Mitte 2007 von LookSmart übernommenen Web Crawler Grub (www.grub.org) integriert. Außerdem sollen die Benutzer Suchergebnisse bewerten und so deren Qualität verbessern.

Da bislang solche Bewertungen fehlen (unter anderem weil sie noch nicht eingebaut sind), können die Ergebnisse noch nicht gut sein. Zu den Besonderheiten sollen später Kurzdefinitionen zu Begriffen gehören. Schließlich soll eine nutzergepflegte Whitelist (search.wikia.com/wiki/Whitelist) einen Korpus „guter“ (= zu durchsuchender) Sites gewährleisten.

IE 8 und Firefox 3 bestehen Acid2-Test

Nach Safari, Konqueror und Opera sollen die künftigen Versionen von Internet Explorer (V. 8) sowie Firefox (V. 3) ebenfalls den vom Webstandards-Projekt (www.webstandards.org/action/acid2/) erstellten CSS-Test bestehen, der unter dem Namen Acid2 bekannt ist. Wie untenstehende Abbildung zeigt, handelt es sich darum, Eigenschaften von CSS 2.1 korrekt in einen Smiley samt Beschriftung umzusetzen. Dazu gehören transparente PNGs, das Box-Modell und Tabellen – und ein paar „illegale“ CSS-Statements, die „gute“ Browser zu übergehen haben.



Robuster 8,4"-Tablet-PC mit LED-Backlight

Ein extrem robuster mobiler Begleiter soll der neue Tablet-PC Tetralight E100 von Logic Instrument sein. Er ist mit einem 8,4"-SVGA-TFT-Touchscreen ausgestattet, das mit LED-Hintergrundbeleuchtung arbeitet und eine Leuchtkraft von über 1000 cd/m² erreichen soll, ohne dabei den Akku allzu sehr zu belasten. Eine reflexionsarme Display-Oberfläche und eine automatische Helligkeitsregulierung sollen die Lesbarkeit in schwierigen Umgebungen von praller Sonne bis zum finsteren Keller gewährleisten.

Der Tablet-PC des französischen Herstellers von robusten portablen PCs basiert auf der von Intel 2007 vorgestellten McCaslin-Plattform für Ultra Mobile PCs (UMPCs), bestehend aus dem 945GU-Chipsatz und einem A110-Prozessor, in dem sich ein mit 800 MHz getakteter Dothan-Kern mit auf 256 KByte beschnittenem L2-Cache verbirgt. Bedient wird die CPU von einem bis zu 1 GByte großen Arbeitsspeicher, als Schnittstellen stehen USB-2.0- und Gigabit-Ethernet-Ports, Anschlüsse für Kopfhörer und Mikrofon sowie ein PCMCIA-Steckplatz für UMTS-, Bluetooth-, GPS- oder WLAN-Module bereit.

Vorinstalliert auf einer stoßsicher gelagerten Festplatte mit Kapazitäten von 40 bis 160 GByte oder einer SSD (Solid State Disk) ist entweder eine Windows XP Tablet Edition oder eine Vista Business Edition. An der Linux-Kompatibilität arbeitet der Hersteller momentan noch.

Ohne Zusatzoptionen wiegt der lüfterlose Tablet-PC etwa 1,3 kg und soll auf eine Akkulaufzeit von bis zu sieben Betriebsstunden kommen. Sein Magnesium-Leichtmetall-Gehäuse entspricht nationalen und internationalen Zulassungsbedingungen und Robustheitsnormen wie CE/FCC Klasse B, UL, MIL-STD-810F und IP54. Der Tetralight E100 arbeitet im Temperaturbereich von - 20° C bis + 60° C bei einer Luftfeuchtigkeit von 10 bis 90 %. Stürze aus 90 cm Höhe soll er laut Hersteller schadlos überstehen. Kfz-Halterungen lassen sich projektbezogen an jeden Fahrzeugtyp anpassen. Ein Crashtest-Gutachten des TÜV gestattet die Montage der Halterungen im Sichtfeld des Fahrers. Der Nettopreis beginnt bei 2600 Euro.



In praller Sonne ebenso wie im Keller soll der 8,4"-Touchscreen mit LED-Backlight des robusten Tablet-PCs Tetralight E100 lesbare Bildschirminhalte produzieren.

Notebook-Platten mit 320 und 500 GByte

Auf der CES hat Hitachi zwei 2,5"-SATA-II-Festplatten mit jeweils 500 oder 400 GByte vorgestellt. Die Travelstar 5K500 für Notebooks und die Travelstar E5K500 für den 24-Stunden-Betrieb in Bladeservern, Routern, Point-of-Sale-Terminals und Videoüberwachungssystemen arbeiten mit Perpendicular Magnetic Recording (PMR) auf drei Magnetscheiben. Gegenüber dem 2-Scheiben-Vorgänger mit 250 GByte hat sich der Energieverbrauch nur unwesentlich auf 1,9 Watt im Schreib-/Lese-Betrieb und 0,9 Watt im Leerlauf erhöht. Die Travelstar 5K500 soll ab Februar 2008, die E5K500 am Ende des zweiten Quartals 2008 erhältlich sein.

Auf ähnliche Verbrauchswerte kommen die 2,5"-Modelle der neuen MHZ2-BH-Serie von Fujitsu mit Kapazitäten von 40 bis 320 GByte, die ebenfalls mit PMR arbeiten. Sie benötigen durchschnittlich 0,6 Watt im Leerlauf, 0,13 Watt im Standby-Betrieb und 2,1 Watt im Schreib-/Lese-Modus.

Externe Festplatte mit AES-Verschlüsselung

Maxtor BlackArmor nennt Seagate seine jüngste Schöpfung, eine portable USB-2.0-Festplatte mit 160 GByte Speicherkapazität und hardwarebasierter AES-Verschlüsselung. Anders als Softwarelösungen verlagert sie alle Produkt-Keys und Verschlüsselungsprozesse direkt auf die Festplatte und lässt sich auch für den Neueinsatz oder die Ausmusterung der Festplatte nutzen. 208 Gramm soll das 2,5"-Laufwerk samt externem Gehäuse wiegen und ab dem zweiten Quartal 2008 für etwa 150 US-Dollar brutto erhältlich sein. Vorinstalliert ist die Maxtor Manager Software Suite für automatische Backups und zur Datensynchronisierung.

Solid State Disk mit 128 GByte

Auf 128 GByte hat Samsung die Schallmauer der SSD-Kapazität geschoben. Die auf der Consumer Electronics Show (CES) in Las Vegas vorgestellten Solid State Disks arbeiten mit Multi Level Cells (MLC) genannten Flash-Modulen und sollen eine Schreibgeschwindigkeit von 70 MByte/s und eine Lesegeschwindigkeit von 100 MByte/s über das SATA-II-Interface erreichen. Letzteres unterstützt neben dem üblichen Native Command Queuing (NCQ) und Spread-Speed Clocking ein Device/Host-initialisiertes Power-Management, das den Stromverbrauch auf 0,5 Watt im Active Mode senkt.

Geplant ist eine 128-GByte-SSD-Version im üblichen 2,5"-Format für Notebooks, eine „Thin-Standard“-1,8"-Version mit einer Höhe von 5 mm für Ultra-Mobile-PCs (UMPCs) sowie eine konventionelle 1,8"-Version für mobile Konsumer-Geräte. Beginnen will Samsung mit der Massenfertigung der 128-GByte-SSDs in diesem Halbjahr. Preise sind noch nicht bekannt.

Auch Toshiba hat bereits für die erste Jahreshälfte eine 128-GByte-SDD mit einer Geschwindigkeit von 100 MByte/s lesend und bis zu 40 MByte/s schreibend in Aussicht gestellt. Sie soll etwa 800 US-Dollar kosten.

Erster Wireless-USB-Grafikadapter

DisplayLink und Alereon haben auf der Consumer Electronics Show (CES) ein Referenzdesign für Bildschirm-Adapter mit Wireless-USB vorgestellt. Es kombiniert den durch die Worldwide WiMedia Alliance zertifizierten AL5000-Chipsatz von Alereon mit der Netzwerk-Display-Technik von DisplayLink. Der Prototyp arbeitet mit Wireless-USB und erreicht UWB-Geschwindigkeiten (Ultra-Wideband) mit einem standardisierten Wireless-USB-Input und Output-Auflösungen bis 1680 × 1050 und 16,7 Millionen Farben – also 24 Bit – mit ruckelfreier DVD-Videowiedergabe.

Der AL5000 enthält alle maßgeblichen Funkschaltkreise, darunter Synthesizer VCO/PLL, Anti-Alias-Filter, LNAs und Transmit/Receive-Switches, Media Access Controller (MAC) und Baseband Processor (BBP) und deckt die gesamte WiMedia-Bandbreite von 3,1 bis 10,6 GHz ab. Alereon liefert den Chip gemeinsam mit der Firmware und allen zur Entwicklung von Wireless-USB-Produkten benötigten Softwaretreibern aus.

Dazu gesellen sich Network-Display-Chips mit einer Hardware Rendering Engine (HRE) und einer VCC-Software (Virtual Graphics Card), die 32-Bit-Grafiken mit Echtzeit-Video-Wiedergabe über USB, Wireless-USB, Ethernet oder WLAN an Monitore, videofähige USB-Laptop-Docking-Stations, Skype-Video-Telefone, Foto-Displays und andere Geräte übertragen.

Mit dem Referenzdesign sollen Hersteller von PC-Komponenten eigene Adapter für Wireless-Bildschirme mit hoher Bildqualität entwickeln können. Die WiMedia-Zertifizierung soll sicherstellen, dass die damit produzierten Produkte kompatibel sind mit zukünftigen USB-fähigen Notebooks.

Fehlersuche in Multi-Threaded-Anwendungen

Coverity hat eine neue Version von Prevent, seinem Produkt zur Codeanalyse in C/C++ und Java, vorgestellt. Entwickler von Multi-Threaded-Anwendungen können über das Interface komplexe Überlappungen ihrer Programme festellen und Datenverletzungen aufgrund von Race Conditions ebenso vermeiden wie Deadlocks oder Performance-Einbußen, die durch sogenannte Thread Blocks verursacht werden. Der Preis von Coverity Prevent hängt laut Hersteller vom Projektumfang ab (www.coveri ty.com).

Rich-Internet-Anwendungen mit JViews 8.1

Kürzere Ladezeiten und schnellere Seitenaktualisierungen verspricht Ilog Webentwicklern, die die aktuelle Version von JViews einsetzen (www.ilog.com/products/jviews/). Die für High-End-Visualisierung konzipierte Software unterstützt Ajax und erlaubt die direkte Bearbeitung von Diagrammen, Charts und Karten im Webbrowser. Für schnellere Reaktionszeiten hat der Hersteller unter anderem die Grafik-Engine optimiert. Neu ist die Graph-Layout-Komponente für das Eclipse Graphical Editing Framework (GEF), die miteinander verbundene Elemente wie Netzstrukturen oder Geschäftsprozessdiagramme automatisch platziert.

Neue Flash-Server von Adobe

Ohne lizenzrechtliche Einschränkungen lassen sich mit dem Flash Media Streaming Server 3 qualitativ hochwertige, verschlüsselte Videos übertragen, sowohl on demand als auch in Echtzeit. Der darauf aufbauende Interactive Server unterstützt eine neue Plug-in-Architektur und ist in Rechtemanagement-Systeme für Zugriffskontrollen in Echtzeit integrierbar. Beide Server unterstützen den Videostandard H.264 und das Audioformat HE-AAC im Flash Player 9, der mittlerweile den Beta-Status verlassen hat.

Adobe bietet den Flash Media Interactive Server 3 für rund 4800 € an. Der Streaming Server soll etwa 1000 € kosten (www.adobe.com./products/flashmediaserver/).

KURZ NOTIERT



Maya lässt Muskeln spielen: Für seine Animationssoftware Maya 2008 bietet Autodesk die Extension 1 an (www.autodesk.com/maya-extension1). Das vor Kurzem von Comet Digital erworbene System enthält Funktionen, mit denen sich Muskel und Haut digitaler Figuren realistisch modellieren und animieren lassen.

Neue Grafikprozessoren von Nvidia: Quadro FX 3700 soll die doppelte Leistung seines Vorgängers bieten. Mit 112 parallelen Prozessoren, 512 MByte Grafikspeicher und einem 256-Bit Speicherinterface ist der High-End-Grafikprozessor speziell für interaktive Visualierungen im Bereich CAD konzipiert. Das neue Modell ist ab 859 € erhältlich. In der Preiskategorie um 300 € hat der Hersteller das Geforce-Modell 8800 GTS mit 512 MByte Videospeicher vorgestellt, das 25 Prozent mehr Performance als seine Vorgängermodelle bringen soll (www.nvidia.de/wheretobuy).

Neues SDK für Perforce: Speziell für individuelle ALM-Lösungen hat Perforce das Software Development Kit für sein Softwarekonfigurations-Managementsystem konzipiert (www.perforce.com). Das SDK ist eine Ergänzung des Defect Tracking Gatewayzur Anbindung von Anwendungen zur Fehlerüberwachung.

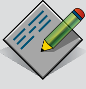
Bull führt Nagios-Überwachung ein

Im Rahmen ihrer Opencenter-Lösungen, einem modular aufgebauten Konzept von Open-Source-Software, hat Bull ein Dienstleistungspaket zur Systemüberwachung mit Nagios geschnürt. Auf einem oder mehreren Servern laufen Linux, ein Apache-Webserver und Nagios. Die zu überwachenden Systeme melden ihren Systemstatus mittels Agenten an die Nagios-Konsole. Die grafische Aufbereitung der erfassten SNMP- und Auslastungsdaten übernimmt die Oberflächensoftware Cacti. Zu den von Bull offerierten Services zählen die Definition der zu überwachenden Umgebung, das Konzept für Geräte, Gruppierung, Benachrichtigungen und Eskalationsprozeduren sowie die Grundinstallation der Software einschließlich Realisierung einer Basisprüfung, Tests und abschließender Einweisung der Systemverantwortlichen. Das Basispaket umfasst die Überwachung von bis zu zehn Servern (Windows, Linux, AIX, HP-UX oder Sun). Der Preis beträgt 5000 Euro.

Virtualisierungsfan EMC

Einen neuen Anlauf unternimmt EMC in Sachen SAN-Virtualisierungssoftware. Gegenüber der Vorgängerversion soll Invista 2.0 die doppelte Anzahl an virtuellen Volumes und Speicherelementen innerhalb eines Speichernetzes verarbeiten sowie das Fünffache an Speicherressourcen gleichzeitig bewegen können. Mit der Software lassen sich verteilte physische Speichersysteme in einem gemeinsamen logischen Pool nach Speicherebenen klassifizieren. Neue verteilte Control Path Clusters (CPC), deren Verbindungspunkte bis zu 300 Meter voneinander entfernt sein dürfen, sollen die Verfügbarkeit verbessern. Die Integration von EMCs Recoverpoint erlaubt zudem Datenreplikationen zwischen physischen und virtuellen Volumes. Invista unterstützt unter anderem Switches von Brocade mit 4-GBit-FC, DS400-Speicher von IBM und Suns MPxIO-Server.

KURZ NOTIERT



Identitätshandel: Quest Software hat Passgo Technologies übernommen, einen Anbieter von Zugriffs- und Identitätsmanagement aus Großbritannien. Mit dem Kauf weitet Quest das Portfolio für die Benutzerverwaltung und die Zugriffskontrolle neben Microsofts Active Directory auf Unix sowie Plattformen wie IBMs zSeries- und iSeries-Systemen aus.

Eingebaut: SAP-Spezialist Realtech macht es möglich, Verfügbarkeits-, Performance- und Fehlerstatus einer beliebigen Netweaver-Komponente in Echtzeit in Microsofts System Center Operations Manager 2007 anzuzeigen. Die Preisliste für das entsprechende Management-Pack for SAP Monitoring startet bei 9950 Euro.

SOA-Kurs: Consol will auf der Cebit einige Neuerungen an seiner Helpdesk-Software Consol CM vorführen. Wichtigste Neuheit ist die serviceorientierte Architekturplattform, die eine Anbindung an Anwendungsprogramme erleichtern soll. Darüber hinaus unterstützt die Business-Intelligence-Funktion nun eine sekundenschnelle Adhoc-Datenanalyse.

Leopard gezähmt: Brainworks' jüngste Version 4.6 der Systemmanagement-Lösung LANrev versteht sich jetzt bestens mit Mac OS X 10.5. Durch den direkten Zugriff auf Time-Machine-Backups lassen sich Clients zentral per Mausklick wiederherstellen. Außerdem nutzt die Admin-Konsole die Screen-Sharing-Software von Mac OS. Administratoren steuern damit die Bildschirme der gewünschten Rechner.

Bedienkomfort: Das Äußere zählt

Laut einer Untersuchung von Forrester Consulting sollten Anbieter von Unternehmenssoftware bei der Gestaltung von Benutzeroberflächen sorgfältiger vorgehen. Denn 82 Prozent der rund 230 befragten CIOs und IT-Leiter lassen sich beim Kauf neuer Software von deren Erscheinungsbild leiten. Bei Update-Fragen halten dies sogar 90 Prozent für das entscheidende Kriterium. Ausschlaggebend ist der vermutete Zusammenhang zwischen Oberflächenqualität und Produktivität. Für 86 Prozent der IT-Manager verursacht eine stressfreie Bedienung die ausgeprägtesten Produktivitätsschübe. 84 Prozent der Befragten sind überzeugt, dass eine gut gestaltete Anwendung zu weniger Fehlern führt. In Auftrag gegeben hatte die Untersuchung die US-Firma Lawson, die im Frühjahr vergangenen Jahres ihrer eigenen ERP-Software M3 ein neues Äußeres spendierte.

Neue Sugar-Release ist fertig

SugarCRM hat die Release 5.0 seines CRM-Produktes freigegeben. Die Software für das Kundenbeziehungsmanagement erhielt beispielsweise einen Ajax-E-Mail-Client sowie bessere Darstellungsfunktionen. Die Zugangskontrolle lässt sich nun für Teamhierarchien bis zu Informationen auf Feldebene eingrenzen. Ein Module Builder ermöglicht das Erstellen eigener Module sowie die Einbindung benutzerdefinierter Objekte in ein Modul. Gleichzeitig präsentierte das Unternehmen seine On-Demand-Architektur. Angeblich ist der Wechsel zwischen Eigenbetrieb und der On-Demand-Variante jederzeit möglich. Interessierte können sich die nach GPLv3 lizenzierte Sugar Community Edition 5.0 bei www.sugarforge.org/content/downloads/ herunterladen. Eine ebenfalls kostenlose Probeversion von Sugar Professional 5.0 On-Demand liegt unter www.sugarcrm.com.

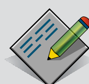
E2E erweitert Middleware

Das Schweizer Unternehmen E2E hat seine E2E Bridge, eine Lösung für die modellbasierte Integration, erweitert. Neben UML arbeitet die Middleware nun mit weiteren Modellierungssprachen zusammen, darunter BPMN (Business Process Modeling Notation) und EPK (Ereignisgesteuerte Prozesskette). Das Softwarehaus bietet die jüngste „Brücken“-Generation in vier vorkonfigurierten Varianten für unterschiedliche Anwendungsfälle an: Hochskalierbar, On Demand/SaaS, BPM und Integration über Schnittstellen.

Bea: Roadmap für Genesis

Im zweiten Quartal dieses Jahres will Bea eine SaaS-Plattform (Software as a Service) für Unternehmen als erstes Produkt seines Genesis-Projekts auf den Markt bringen. Für unabhängige Softwareanbieter soll sich damit das Entwickeln neuer Produkte wesentlich einfacher gestalten. Angeblich lassen sich vorhandene Anwendungen und Architekturen einfach in die neue Plattform integrieren, Open-Source-Software inklusive. Laut Bea wird Genesis die Art, wie Geschäftssoftware erstellt wird, radikal ändern.

KURZ NOTIERT



Aufgepeppt: SAP hat sein CRM 2007 vorgestellt. Das Produkt enthält eine Reihe zusätzlicher Funktionen und Erweiterungen. Angebote sollen sich nun beispielsweise in Echtzeit abwickeln lassen. Weiterentwickelt hat SAP die Software auch in den Bereichen Verkaufsförderung, Kundenkommunikation und Controlling. Die Bedienoberfläche ist ebenfalls neu und verfügt über Web-2.0-Funktionen.

Ausgeweitet: Das bislang nur für Swing-Anwendungen erhältliche Testwerkzeug QF-Test der QFS aus Geretsried lässt sich in der Version 2.2. auch in der Eclipse-Plattform einsetzen. Anwender können ihrer Eclipse-SWT- und RCP-Programme mit dem Tool automatisiert testen. Eine frei übertragbare QF-Test-Lizenz kostet unter 2000 Euro. Bei höheren Stückzahlen vergibt das Unternehmen Lizenzen zur Miete.

Umgetauft: Die Münchner Softlab Group hat sich in Cirquent umbenannt. Ziel der Aktion ist es, die verschiedenen Marken des Hauses zu bündeln. Das Kunstwort Cirquent setzt sich aus den Begriffen „Circle“ und „konsequent“ zusammen. Man positioniert sich jetzt klar als Beratungshaus für Banken, Versicherungen, Telekommunikationsunternehmen und Fertigungsindustrie.

Talentsicht: SAP schloss ein weltweites Wiederverkäuferabkommen mit dem kanadischen Unternehmen Nakisa. Danach wird SAP HCM (Human Capital Management) Funktionen aus Nakisas Mitarbeiterverwaltung übernehmen. Sie helfen bei der Darstellung der Organisation sowie beim Talentmanagement für die Besetzung von Schlüsselpositionen. SAP vermarktet die Anwendung unter dem Namen „Talent Management Visualization by Nakisa“. Nakisa enthält im Gegenzug eine Finanzspritze aus dem SAP Netweaver Funds.

Zur Miete: Seit Dezember ist Sage hierzulande im SaaS-Geschäft (Software as a Service) aktiv. Für das gehostete Sage-CRM möchte der Anbieter 21 Euro pro Monat kassieren. Die Lösung verfügt über Funktionen zum Erstellen von Umsatzprognosen und Berichten, zum Kampagnenmanagement sowie zum Steuern von Werbemaßnahmen. Sie lässt sich mit Outlook synchronisieren und in die Office-Line von Sage einbinden.

Nur einmal: Infostore Release 9 der SoftM-Tochter Solitas unterstützt die sichere Archivierung auf handelsüblichen Festplatten. Die SnapLock-Technik verwandelt die Harddisk dazu in ein einmal beschreibbares Medium. Ein spezieller Server, der neben den klassifizierten Dokumenten auch die Informationen aus der OCR-Erkennung verwaltet, reichert die für IBM iSeries verfügbare Lösung mit Volltext-Retrieval an. Neu ist zudem das Signatur-Modul für die Einbindung von Verschlüsselungsdiensten verschiedener Signatur-Provider.

Eingekauft: EMC übernimmt die Document Sciences Corp., einen Anbieter für sogenannte Document-Output-Management-Lösungen. Diese ermöglichen die personalisierte Massenkommunikation mit Kunden über unterschiedliche Kanäle. Der Deal soll im ersten Quartal dieses Jahres über die Bühne gehen; der Kaufpreis beträgt rund 85 Mio. Dollar.

Kleiner Einstieg: Hierzulande soll es mehr als 2,8 Mio. Unternehmen mit weniger als 50 Mitarbeitern geben. Diese will Microsoft mit der ERP-Software „Dynamics Entrepreneur“ beglücken. Sie basiert auf dem „großen“ Dynamics NAV (vormals Navision). In der Mini-Variante ist die Software für maximal fünf gleichzeitig arbeitende Nutzer ausgelegt. Im Januar will Microsoft Einzelheiten zum Vertriebskonzept bekanntgeben.

Web-2.0-Zugabe: Alfresco Software erweitert die gleichnamige quelloffene ECM-Software um eine Social Computing-Plattform. Das neue Paket reichert das Ursprungsprodukt mit Web-2.0-Tools an und bietet Anschluss an Dienste wie Facebook, iGoogle, Adobe Flex, Mediawiki, Typepad und Wordpress.

Artix mit Open-Source-Anleihen

Iona hat eine aktualisierte Version der quelloffenen SOA-Produktfamilie Fuse vorgestellt, die auf verschiedenen Apache-Projekten basiert. Dazu gehören ein ESB (ServiceMix), ein Message Broker (ActiveMQ), ein Services Framework (CXF) sowie der Mediation Router (Camel). Fuse ist der Nachfolger der SOA-Software Celtix des irischen Anbieters.

Die Release umfasst erstmals Fuse HQ, das Systemmanagement- und Monitoring-Fähigkeiten für alle Produkte der Familie bereitstellt. HQ basiert auf Hyperic HQ Enterprise und ist nur im Zusammenhang mit Support von Iona verfügbar. Es stellt eine Webmanagementkonsole zur Verfügung und bietet weiterhin Plug-in-Agenten für alle anderen Komponenten, globale Konfiguration von Ansichten, Metriken und Alarm, regelbasierte Zugangskontrolle und optional ausführbare „Kontrollaktionen“ sowie verteiltes Monitoring.

Der Anbieter spricht von einem hybriden Ansatz, denn wenn ein Unternehmen weiterführende Fähigkeiten benötigt, muss es auf ein kommerzielles Produkt zurückgreifen. Hier hat Iona natürlich seine SOA-Produktsuite Artix im Sinn, deren Governance-, Management- und Interoperabilitätsfähigkeiten die Firma erweitert hat. Zu den Neuigkeiten zählt beispielsweise ein Versionsmanagement für Services und andere Repository-Artefakte. Das Datenmodell des Repositories lässt sich nun anpassen; die Services kann man in einer UDDIv3-Registry veröffentlichen.

Susanne Franke

IT-Trends im deutschen Maschinenbau

Nach Einschätzung von IDC haben IT-Anbieter derzeit bei den deutschen Maschinenbauern gute Chancen. Allerdings müssen sie fundierte Kenntnisse über die speziellen IT-Erfordernisse der Branche nachweisen können. Beispielsweise erzeugt die wachsende Konkurrenz aus Niedriglohnländern Nachfrage nach neuen technischen Funktionen. Diesem und ähnlichen Themen widmet sich die Studie „IT-Trends im deutschen Maschinenbau“, die sich gezielt an Hersteller richtet.

Im Mittelpunkt aller Bemühungen sehen die Marktforscher einen hochwertigen Kundenservice. Verbesserungsbedarf besteht etwa bei der Konsolidierung der entsprechenden Kundendatenbanken. RFID und eine standardisierte IT sollen die Fertigungsprozesse und die Lieferkette optimieren. Eigenentwicklungen und isolierte Applikationen wollen die Unternehmen abschaffen. Für die Untersuchung befragte IDC 52 IT-Verantwortliche aus großen sowie mittelständischen Maschinenbauunternehmen. Die Studie kostet 3900 Euro.

Barbara Lange

Archive für die Ewigkeit

Die Archivierungslösungen von Open Text halten sich an den neuen Standard zur Langzeitarchivierung Evidence Record Syntax (ERS), alias RFC-4998. Darüber sollen Unternehmen das Problem der rechtssicheren Langzeitarchivierung durch die Erneuerung von Signaturen lösen (siehe Seite 128 in diesem Heft). Es ist gesetzlich vorgeschrieben, dass Firmen und öffentliche Stellen ihre Dokumente im Zeitverlauf mit immer stärkeren Algorithmen beziehungsweise längeren Schlüsseln schützen müssen. Mithilfe von ERS können sie für jedes archivierte Dokument ein sogenanntes Beweisdokument (Evidence Record) bilden. Es stellt sicher, dass sowohl das Dokument als auch die verwendeten Signaturen vor ihrem Verfallsdatum existierten und seitdem nicht verändert wurden. Bei der Entwicklung der im August 2007 verabschiedeten Spezifikation war Open Text federführend beteiligt. Der IETF-Standard beruht auf den Ergebnissen des vom Bundesministerium für Wirtschaft und Arbeit geförderten ArchiSig-Projekts.

Onlinewerbung: Die Milliarde im Blick

Der Umsatz mit grafischer Werbung auf Webseiten hat sich laut einer Meldung des Bitkom in Deutschland 2007 auf 976 Mio € gegenüber dem Vorjahr verdoppelt. IT-Anbieter und Internet-Plattformen gaben rund 223 Mio. € für Onlinewerbung aus. Auf dem zweiten Platz folgten Handels- und Versandhäuser, die 189 Mio. € investierten. Medien und Entertainment-Anbieter (119 Mio. €), Banken und Finanzdienstleister (116 Mio. €) sowie Kfz-Firmen (89 Mio. €) gelten ebenfalls als Branchen mit Affinität zur Onlinewerbung.

Eine untergeordnete Rolle spielte diese Form der Werbung hingegen für die Pharmaunternehmen (6,5 Mio. Euro). Sie favorisieren stattdessen klassische Formen wie Werbespots im Fernsehen sowie Anzeigen in Zeitungen und Zeitschriften. Grundlage des Zahlenwerks ist eine Untersuchung des Marktforschungsinstituts Thomson Media Control, auf die sich der Bitkom beruft.

Die Angaben umfassen allein klassische Onlinewerbung (Banner, Popups und Streaming Ads). Suchwort-Marketing und Affiliate-Marketing sind nicht eingeschlossen, weswegen der Bundesverband Digitale Wirtschaft (BVDW) bereits die Zahlen für 2006 für zu niedrig angesetzt hielt. Ausgewiesen ist allein der hochgerechnete Nettoumsatz. Rabatte und Agenturprovisionen sind also berücksichtigt.

3Com-Kauf später

Die Genehmigung des Kaufs von 3Com durch den Finanzinvestor Bain Capital sowie den chinesischen Kommunikationskonzern Huawei verzögert sich. Das hat die zuständige US-Regierungsbehörde CFIUS (Committee on Foreign Investment in the United States) signalisiert. Auslöser der intensiven Prüfung ist die Zusammenarbeit von 3Com mit dem Pentagon. Auch wenn Huawei nur 16,4 % der Anteile erwerben will, befürchtet man, dass chinesische Spezialisten Einblick in sicherheitskritische Techniken (z. B. Intrusion-Prevention-Systeme) des US-Verteidigungsministeriums erhalten. Bain und Huawei wollen für 3Com rund 2,2 Mrd. Dollar springen lassen.

Infoexchange@ca: Ein Managementbild mit vielen Facetten

IT-Governance war eines der Hauptthemen der zweitägigen Anwenderkonferenz von CA. Schließlich gilt es, das Management und die Steuerung der IT-Ressourcen an Geschäftsprozessen und Services auszurichten. Dazu trägt jede Managementdisziplin ihr Scherflein bei.

„Es geht nicht mehr allein darum, einzelne IT-Komponenten zu managen“, erläuterte Dr. Ajei Gopal, verantwortlicher Manager für die Management- und Sicherheits-Geschäftssparte bei CA, in seinem Eröffnungsvortrag zur diesjährigen Infoexchange den Unterschied zum bisherigen System- und Netzwerkmanagement. Er entwarf ein Bild des künftigen IT-Managements, das die heute noch meist getrennten Management-Disziplinen zusammenführt. Im Mittelpunkt steht nach Überzeugung Gopals in Zukunft die Verwaltung eines Service-Portfolios inklusive der unterliegenden IT-Ressourcen. Auf diese Weise sei es möglich, jederzeit Einblick in deren Qualität und Kosten zu erhalten.

CA setzt im Unterschied zur Strategie anderer Anbieter auf das Konzept des EITM (Enterprise IT Management), das die IT unternehmensweit steuert, verwaltet und sichert. Dabei folgt die US-Firma dem Ansatz, eine Gesamtsicht auf die IT-Services entlang ihres Lebenszyklus zu liefern. Vom Service-(Qualitäts-)Management bis zur Infrastrukturoptimierung und Rechenzentrumsautomatisierung greifen die unterschiedlichen Verwaltungsebenen ineinander. So lassen sich beispielsweise die Speicher-, Anwendungs- und Serverressourcen und -virtualisierungsfunktionen zu dem Zweck kombinieren, einen Service vollständig zu virtualisieren. Änderungen an den Services führen dann automatisch zu Anpassungen der Ressourcen.

Gopal skizzierte, wie die CA-Produkte und -Akquisitionen aus der Vergangenheit einen solchen Ansatz mit Leben füllen. Die Projektportfolio-Managementlösung Clarity wird beispielsweise zu einem Serviceportfolio-Management ausgebaut, um die Investitionen in IT-Services und nachgelagerte Infrastruktur aus der Perspektive der Geschäftsanforderungen zu entscheiden. Mithilfe von Wily Introscope wird wiederum die Leistung und Qualität der IT-Services und komplexen Webumgebungen auf Anwendungsebene überwacht, während Unicenter NSM und Concord/Spectrum diese Aufgabe für die System- und Netzwerkebenen übernehmen. Abgesichert wird das Ganze durch Netegrity, das einen Sicherheitsdomänen-übergreifendes Zugriffs- und Identitätsmanagement realisiert.

Wie weit die Umsetzung im Einzelnen gediehen ist, konnten die Teilnehmer in weiteren Vorträgen und in der begleitenden Ausstellung der Infoexchange@ca erfahren. Vorgestellt wurde unter anderem CA IAM r12, die nun auch Identitäts- und Zugriffsmanagement, Workflow-Automatisierung, delegierte Administration, Reporting sowie Federation-Funktionen für Webservices und auf serviceorientierten Architekturen (SOA) basierende Geschäftsabläufe bietet. Zu begutachten war des Weiteren die Beta-Version einer Automatisierungslösung für den Rechenzentrumsbetrieb, der Data Center Automation Manager (DCA Manager). Das Werkzeug automatisiert regelbasierend den Prozess, IT-Ressourcen gemäß den Anforderungen zu provisionieren. Melden beispielsweise die Performance-Agenten das Überschreiten eines definierten Schwellwertes für einen IT-Service, öffnet der DCA automatisch ein Trouble Ticket, um das Problem detaillierter zu analysieren. Über CA Cohesion erhält das Werkzeug wiederum Informationen zu Blaupausen oder „bewährte“ Server-Konfigurationen. Mit diesem Wissen lassen sich dynamisch neue Ressourcen zuordnen, um die Qualitätsvorgabe für den IT-Service wiederherzustellen.

AOL verabschiedet sich vom Web-Urgestein Netscape

Zum 1. Februar zieht AOL den Schlussstrich unter einen 4,2 Mrd. Dollar teuren Irrtum. Netscapes Webbrowser Navigator wird nicht mehr weiterentwickelt und der Support auslaufen. Verbliebenen Anwendern raten die Entwickler und Manager, auf Firefox umzusteigen. Der Navigator, 1994 aus einem Uniprojekt entstanden, war einmal das „Fenster“ ins World Wide Web schlechthin.

Der Einstieg von Microsoft, insbesondere die später kartellrechtlich abgestrafte Bündelung des Internet Explorer mit Windows sowie dessen freie Abgabe, knabberte an der Marktposition. Netscape rettete sich 1998 in die Arme von AOL. Zuvor hatte man bereits das Open-Source-Projekt Mozilla ins Leben gerufen, die Basis von Firefox.

Unter AOL, insbesondere nach der Fusion mit Time Warner, tat sich nicht mehr viel bei Netscape. Nachdem man 2003 immerhin 750 Mio. Dollar von Microsoft als „Friedensgabe“ erhalten hatte, verabschiedete sich das Unternehmen komplett aus der aktiven Entwicklung. Nun folgt mit der Einstellung des Supports der letzte Schritt. Die bisherigen Netscape-Versionen sollen aber weiter zum Download verfügbar sein.

Kostbare Suche für Unternehmen

Microsoft lässt es sich 1,2 Mrd. US-Dollar kosten, den Suchmaschinenspezialisten Fast Search & Transfer zu kaufen. Das norwegische Unternehmen entwickelt Suchmaschinensoftware für den Einsatz in Unternehmen. In diesem Segment müht sich die Nicht-mehr-Gates-Firma seit Kurzem, mit neuen Releases der eigenen Suchserver Fuß zu fassen. Nach Ansicht von Analysten wie Ovum fehlt es jedoch im Vergleich zu den „High-end“-Anbietern Autonomy, Endeca oder eben Fast noch an Funktionsumfang und Integrationsstärke. Der Preis mutet irritierend hoch an, da die Norweger in den ersten neun Monaten des laufenden Geschäftsjahres einen Umsatz von 119 Mio. Dollar bei 125 Mio. Dollar Verlust erzielten. Ein Mitte 2007 verkündetes Restrukturierungsprogramm soll 2008 die Rückkehr in die Gewinnzone bewirken. Die Fast Enterprise Search Platform lässt sich in die Suchfunktionen von Microsofts Sharepoint Server 2007 einbinden.



Internet billiger: Die Kosten für die Internetnutzung lagen nach Mitteilung des Statistischen Bundesamtes 2007 um 5,3 % unter dem Niveau des Vorjahres. Das Mobiltelefonieren verbilligte sich um 2,4 %. Dagegen legte der Preisindex für Telefondienstleistungen im Festnetz um 1,7 % zu. Dadurch lag der Preisindex für alle drei Bereiche aus Sicht privater Haushalte um 0,4 % über dem Vorjahresniveau.

Ins Netz der Dinge mit Routing-Agenten

Intelligente Routing-Agenten sollen Transportsystemen die Fähigkeit verleihen, Güter schnell und zuverlässig ans Ziel zu bringen. Die Technik kann die komplexe Steuerungslogik, Rechner und Datenverarbeitungssysteme zum Beispiel bei Gepäcktransportanlagen in Flughäfen ersetzen. Ziel ist es, das Internet der Dinge zu realisieren, in dem Güter und Steuerungseinheiten miteinander kommunizieren, um selbstständig Entscheidungen über Wege zu fällen und Betriebsmittel anzufordern.



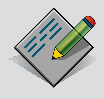
Lauerstellung: An den Weichen überwachen Agenten über RFIDs den Fluss der Güter und handeln mit anderen Agenten den optimalen Weg aus (Abb. 1).

Das Fraunhofer-Institut für Materialfluss und Logistik IML (www.iml.fraunhofer.de) in Dortmund hat zusammen mit dem Lehrstuhl für Förder- und Lagerwesen FLW der Universität Dortmund (www.flw.mb.uni-dortmund.de) das Kommunikationsverhalten an einem konkreten Fall untersucht. Dazu haben die Forscher eine automatische Gepäckförderanlage für Großflughäfen umgerüstet: 2000 Routing-Agenten an den Weichenstellungen steuerten eine Gepäckförderanlage mit 12 000 Förderelementen und 1200 Verzweigungen. Das neue System war dabei in der Lage, auf eine wachsende Zahl von Gepäckstücken zu reagieren und einen Stau zu vermeiden, indem die Agenten alternative Routen aushandelten. Solche Agenten kommen mit einfachem Programmcode aus und können trotzdem die Funktion eines großen Fördersystems sicherstellen.

Notebook mit 1 Terabyte Plattenspeicher

Eine 500 GByte große 2,5-Zoll-Festplatte namens Travelstar 5K500 hat Hitachi Anfang des Jahres vorgestellt und angekündigt, dass Asus die Platten in seinen M50- und M70-Notebooks verwenden will. Auf der Consumer Electronics Show (CES) in Las Vegas will Asus einen Prototyp des M70 als erstes „Terabyte-Notebook“ zeigen, das zwei der 500-GByte-Platten aufnehmen kann. Genauere Angaben zu Leistungsaufnahme, Akkulaufzeit, Gewicht und Preis waren bis zum Redaktionsschluss nicht zu bekommen. Es dürfte sich aber um die Desktop-Ersatzklasse handeln.

KURZ NOTIERT



Vorgriff: Avocents Managementsoftware DSView 3 für physische und virtuelle Maschinen sowie der DRS KVM-over-IP Switch unterstützen das Internetprotokoll IPv6 und sind damit auf die ab 2008 beginnende Umstellung von IPv4 in den Behörden vorbereitet (www.avocent.de).

Im Feld: Zur Simulation von Antennenanlagen gibt es Efield (www.efieldsolutions.com), die Forscher in einem Gemeinschaftsprojekt des Fraunhofer-Chalmers Centre FCC in Göteborg, einiger Universitäten und der Unternehmen SAAB, Ericsson AB und Efield AB entwickelt haben. Anlass war die optimale Ausrüstung der GPS-Antennen der Satelliten in der ESA-Mission „Swarm“, die das Erdmagnetfeld untersuchen sollen.

Sensibel: Auf den Namen LISA hört der Life Science Assistant des Fraunhofer-Instituts IFF. LISA besitzt einen Greifarm mit Tastsinn, damit sie als mechanische Dienerin niemanden verletzt. Sie versteht ganze Sätze und ist in begrenztem Maße lernfähig (www.iff.fraunhofer.de).

Neuerungen in VMwares Enterprise Suite VI 3.5

Große Erwartungen hegten die Anwender von VMwares Infrastructure (VI) auf die nächste Release der Virtualisierungssoftware. Vor allem angesichts neuer Techniken gab es einige Wünsche. Die Entwickler bei VMware haben einiges unternommen, um den Ansprüchen gerecht zu werden.

Der Anbieter der Virtualisierungslösung für x86/x86_64-Systeme VMware hat am 12. Dezember ein großes und lang erwartetes Update auf die Version 3.5 der VMware Infrastructure freigegeben. Fast sämtliche Komponenten haben die Entwickler aktualisiert: Der klassische ESX-Server trägt jetzt die Versionsnummer 3.5 (Build 64607), VirtualCenter die 2.5 und VMware Consolidated Backup die 1.1. Ebenso erhielt der Converter eine Auffrischung, allerdings gibt es ihn zumindest im Live-Mode nicht mehr als Einzelversion, da er als zusätzlicher Baustein in das VirtualCenter integriert ist.

Neue ESX-Version ohne COS

Mit ein paar Tagen Verspätung am 20. Dezember folgte der nagelneue ESX Server 3i (Build 67921). Das „i“ signalisiert eine Neuheit bei VMware: Der Server bildet sämtliche Funktionen eines ESX Server 3.5 ab, kommt jedoch ohne die Servicekonsole (COS) aus. Übrig bleibt ein schlanker Hypervisor von lediglich 32 MByte Größe. ESX 3i kann schnell in Betrieb gehen und auf zertifizierter Hardware vorinstalliert werden. Denkbar sind zum Beispiel ein ESX 3i Hypervisor auf einem Flash-Speicher. Wie den ESX 3.5 kann der Systemverantwortliche ESX 3i via VirtualCenter administrieren und überwachen.

Einige der wichtigsten Neuerungen bei ESX: Es gibt jetzt eine Unterstützung für 10-GBit-Ethernet und Infiniband; Jumbo-Frames und TCP Segment Offload haben Einzug gehalten. Das in der Vergangenheit am meisten monierte holprige Update-Prozedere haben die Entwickler komplett neu geschrieben. VMwares Update Manager vermag komfortabel und automatisiert Patches nicht nur in den ESX Server, sondern auch in die Gäste einzuspielen. Weiterhin kann der Systemadministrator mit dem Update-Manager und dem automatisierten Einsatz von Snapshots im Offline-Modus Updates vor dem Einsatz testen, ohne dabei den produktiven Betrieb zu gefährden, ein von der Community oft gefordertes Feature.

Umzug über Grenzen hinweg

VMotion zum Migrieren kompletter ESX Server ist nicht mehr nur auf einen zentralen Speicher beschränkt, Storage VMotion ermöglicht erstmals die Migration einer laufenden virtuellen Maschine über Speichergrenzen hinweg. Die zugrunde liegende Technik bedient sich einer intelligenten Nutzung von Snapshots und Redo-Logs. Mit der neuen Version des ESX Server sind SATA-Festplatten als Speicherort für virtuelle Maschinen zugelassen. Der maximale Hauptspeicher pro VM hat sich auf 64 GByte erhöht und der des eigentlichen ESX Server auf maximal 256 GByte. Weiterhin gibt es nun Gast-Unterstützung für Windows Vista, Ubuntu und experimentell für Windows Server 2008.

Beim Energieverbrauch wagt VMware einen neuen Schritt und integriert ein Distributed Power Management (DPM), vorerst allerdings experimentell. Dahinter verbirgt sich ein System, das automatisch alle laufenden VMs analysiert, sie auf benötigte ESX Server verteilt und danach kurzerhand nicht benötigte abschaltet. Bei Bedarf aktiviert DPM etwaige ruhende Server wieder und verschiebt festgelegte VMs wieder zurück. Notiz am Rande: Fast zeitgleich mit der Release 3.5 gab SAP die offizielle Unterstützung für ihre Software in virtuellen Maschinen unter ESX bekannt.

Jörg Riether

Sichere Onlinetransaktionen mit Flickercode und Fingerprint

Die Schweizer Firma Axsionics hat ein Verfahren entwickelt, mit dessen Hilfe sich Verbraucher beim Onlinebanking per Fingerabdruck identifizieren können. Siemens IT Solutions und Services implementiert und vertreibt eine auf diesem Verfahren beruhende Lösung. Für sichere Onlinetransaktionen hat der Bankkunde einen Internetausweis, auf dem er den Abdruck eines oder mehrerer Finger hinterlegt. Sobald die Überweisungsdaten an die Bank gesendet wurden, erhält der Kunde einen sogenannten Flickercode, bestehend aus sechs Feldern, die abwechselnd schwarz und weiß blinken. Dieser Code enthält den bei der Bank eingegangenen Überweisungsauftrag und die zugehörige TAN in verschlüsselter Form. Der Wechsel der Farben transportiert die kodierten Informationen.

Das Gegenstück, der Ausweis, enthält neben einem Streifensensor zum Scannen des Abdrucks einen Chip mit Keys zum Entschlüsseln der Informationen sowie einen optischen Sensor zum Lesen der Überweisungsdaten. Zieht der Nutzer seinen Finger über den Streifensensor des Ausweises und hält ihn dann vor den Flickercode, so kann er die Daten des Auftrags überprüfen und die TAN eingeben. Der Fingerabdruck ist nur auf der Karte gespeichert und nicht in einer zentralen Datenbank. Laut Angaben von Siemens testen bereits mehrere Banken in der Schweiz und in Deutschland die Lösung. *Susanne Franke*

Starthilfe für KMU in Sachen Sicherheit

Mit dem Informationspaket „Starthilfe Internet“ will der Verein „Deutschland sicher im Netz“ (DsiN) Geschäftsführer, IT-Verantwortliche und Mitarbeiter von kleinen und mittleren Unternehmen bei der Umsetzung sicherheitsrelevanter Maßnahmen unterstützen. Das auf dem 2. IT-Gipfel der Bundesregierung (siehe S. 9) vorgestellte kostenlose Angebot besteht aus mehreren Komponenten: Schon verfügbar ist das von den DsiN-Mitgliedern Hewlett-Packard, SAP und Utimaco erstellte „Medienpaket für den Mittelstand“, bestehend aus den vier Broschüren – genannt Fibeln – „Kryptologie für Jedermann“, „IT-Sicherheitsrecht“, „Sicheres Programmieren“ und „Faktor Mensch“.

Dazu gehört eine CD-ROM mit der kostenfreien Vollversion der Software Safeguard privatecrypto 2.11.1 der Utimaco Safeware AG für die Verschlüsselung aller Dateiformate und E-Mails. Sie enthält auch Trainingsprogramme, Tests zur Selbsteinschätzung der Datensicherheit, Checklisten und Links. Interessierte können das Medienpaket unter www.sicher-im-netz.de – Menüpunkte „Unternehmen“ und „Starthilfe Internet“ – herunterladen oder bestellen. Als weitere Maßnahmen will der anlässlich des ersten IT-Gipfels im Dezember 2006 gegründete Verein im Jahre 2008 Unternehmen online nach ihren Sicherheitsproblemen befragen und daraus den Bedarf an Sicherheitslösungen ableiten. Geplant sind weiterhin Handlungsempfehlungen für den Mittelstand auf der Basis des internationalen Sicherheitsstandards ISO 27001 und kostenlose Seminare. *Barbara Lange*

TK-Anbieter missachten Datenschutz

Telekommunikationsunternehmen halten sich bei der Vertragsanbahnung nur unzureichend an die Vorgaben des Bundesdatenschutzgesetzes. Vor allem lehnen sie einen neuen Kunden häufig automatisiert ab, allein auf der Basis eines Score-Wertes, der Aussagen über die Bonität und das individuelle Risiko eines Kunden trifft. Diese Praxis ist aber nach § 6a Abs. 1 BDSG nicht zulässig. Das stellte der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Peter Schaar, bei einer Prüfung von 26 Telekommunikations-Unternehmen fest. Schaar bemängelte weiterhin, dass die Betroffenen von diesen automatisch gefällten Entscheidungen noch nicht einmal informiert werden und somit ihre Interessen überhaupt nicht zur Geltung bringen können, was gegen § 6a Abs. 2 BDSG verstößt.

Außerdem speichern die TK-Anbieter die von den Auskunfteien erhaltenen Daten häufig viel zu lange, teilweise über Jahre. Zu bemängeln ist auch die Auskunftspraxis mit wenig aussagekräftigen Standardablehnungen. Nach § 34 BDSG müssen Unternehmen aber die verhinderten Kunden umfassend über gespeicherte personenbezogene Daten informieren. Eine Verletzung der Datenschutzrechte von Telefonkunden in diesem Ausmaß hätte Schaar nicht erwartet. Zunächst setzt er noch auf die „Einsichtsfähigkeit“ der TK-Anbieter. Für den Fall, dass sie die Mängel nicht unverzüglich abstellen, kündigte der oberste Datenschützer aufsichtsrechtliche Maßnahmen an. *Barbara Lange*

Telefonüberwachung: Staat muss bezahlen

Die staatlich angeordnete Überwachung von Festnetz- oder Mobiltelefonanschlüssen verursacht bei den Netzbetreibern hohe Kosten. Jetzt hat das Verwaltungsgericht Berlin entschieden, dass diese hierfür in vollem Umfang entschädigt werden müssen. „Die Richter haben klar gemacht, dass der Staat die Kosten für Überwachungstechnik tragen muss“, kommentiert Bernhard Rohleder, Hauptgeschäftsführer des Branchenverbandes Bitkom. Die Richter sind der Meinung, dass die gesetzlich vorgeschriebene Mitwirkungspflicht der Netzbetreiber bei der Telefonüberwachung nur dann verfassungskonform ist, wenn dafür eine volle Entschädigung gezahlt wird. Das Urteil der Berliner Verwaltungsrichter betrifft nicht die Kostenübernahme für die seit Jahresbeginn stufenweise eingeführte Vorratsdatenspeicherung. Trotzdem erwarten viele Juristen, dass die Netzbetreiber auch hierfür eine Entschädigung einklagen werden, wenn der Gesetzgeber nicht für eine gesetzliche Regelung der Kostenübernahme durch den Staat sorgt. Für die Vorratsdatenspeicherung rechnen Experten mit hohen Kosten – sowohl einmalig für die Einrichtung der Überwachungstechnik als auch jährlich für die dauernde Durchführung der Speicherung. *Tobias Haar*



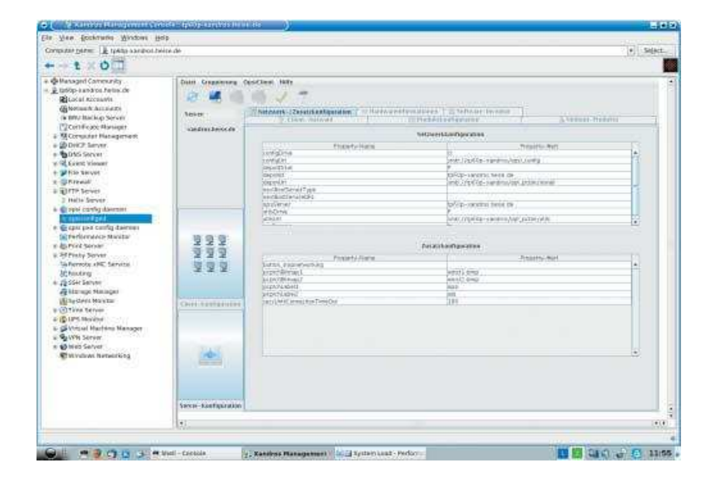
UTM-Geräte: Neue Authentifizierungsmöglichkeiten via Active Directory und Radius bietet die neue Version der UTM-Appliances von Securepoint (www.securepoint.de). Außerdem neu in den Produkten, die standardmäßig mit Firewall-, IDS-, VPN- und Content-Filterfunktionen ausgestattet sind, ist die Validierung von E-Mail-Adressen für SMTP über den Exchange Server.

Daten-Backup: Eine neue Software zur Datensicherung, die auch das Klonen kompletter Festplatten beherrscht, stellt die WAXAR GmbH (waxar.eu) vor. DeviceImage läuft betriebssystemunabhängig auf einer Linux-Boot-CD und unterstützt alle gängigen Filesysteme. Die Software ist vor allem für Backups von großen Festplatten oder Partitionen gedacht.

Windows-Rechner mit Open-Source-Software verwalten

Größere Netze kommen heute ohne geeignete Programme zur Softwareverteilung und zum Remote-Management faktisch nicht mehr aus. Die Mainzer Uib GmbH (Umwelt Informatik Büro, uib.de) hat jetzt von seinem Open-Source-Desktop-Management-Tool Opsi (Open PC-Server-Integration, opsi.org) die Version 3.2 freigegeben. Damit lassen sich über einen Linux-Server, den sogenannten Opsi-Depotserver, via Webservice Windows-Desktop-Systeme verwalten. Opsi bietet neben automatischer Betriebssysteminstallation und Softwareverteilung eine komfortable grafische Management-Schnittstelle sowie Funktionen zur Inventarisierung von Hard- und Software. In der jetzt vorliegenden Version 3.2 haben die Mainzer vor allem die beiden letzten Punkte überarbeitet und erweitert.

Die Wurzeln des Opsi-Projekts reichen bis in die 90er-Jahre zurück. Damals entwickelte Uib das Konzept während eines Projekts für eine Landesregierung, bei dem rund 2000 Clients zentral verwaltet werden sollten. Die Software nebst Dokumentation steht unter download.uib.de/opsi3.2/ zum Download zur Verfügung. Dort liegt auch ein VMware-Image mit einem vorkonfigurierten Opsi-Depotserver, mit dem sich Interessenten ohne großen Aufwand einen ersten Überblick über Opsi verschaffen können. Die Opsi-Basisausstattung ist Open-Source-Software, Uib bietet Support und Schulungen sowie darauf basierende Management-Dienstleistungen an. Für die Cebit arbeiten die Mainzer derzeit an einer – allerdings nur inklusive Maintenance-Vertrag erhältlichen – Version, die sich nahtlos in die grafische Managementkonsole des Xandros Server 2.0 integriert. Auch ein Update der im September für Univentions Corporate Server (UCS) vorgestellten Variante befindet sich in der Testphase.



KURZ NOTIERT

Update: Version 5 des ursprünglich von Red Hat entwickelten Paketmanagers RPM präsentiert sich nicht nur codemäßig gestrafft, sondern kann auch mit LZMA-Kompression und Teilen des XML-Paketformats XAR umgehen. Das Projektteam (rpm5.org) betont, RPM habe sich zu einer Standardmethode entwickelt, Software auf Unix-Systeme zu verteilen.

Lebenszeichen: Parallel zur 2.6-Kernel-Familie pflegen die Entwickler auch den 2.4er-Zweig: Maintainer Willy Tarreau hat den Kernel 2.4.36 freigegeben, der unter anderem über ein neues Sysctl-Item namens *mmap_min_addr* verhindern kann, dass Prozesse die Adresse Null belegen.

Vorschau: Die Samba-Entwickler haben die zweite Alpha-Version von Samba 4 freigegeben. Darin erweiterten sie die Unterstützung für Microsofts Management Console und integrierten Python als zukünftige interne Skriptsprache. Details gibt es unter wiki.samba.org/index.php/Samba4.

Affero GPL Version 3 veröffentlicht

Nachdem die Free Software Foundation (FSF) im Juni 2007 die Version 3 der General Public License (GPLv3) veröffentlichte, erschien Ende letzten Jahres nun Version 3 der Affero GPL (AGPLv3). Bei Letzterer handelt es sich um eine Netzwerkvariante der GPL. Sie basiert auf der GPLv3, hat aber eine kleine entscheidende Ergänzung. Wie schon bei der Affero GPL v2, die auf der Vorgängerversion der GPLv3 beruht, soll die Lizenz Einsatzbereiche von Software erfassen, bei denen es nicht zu einer Vervielfältigung der GPL-lizenzierten Computerprogramme kommt. Wird Software beispielsweise wie bei Software-as-a-Service (SaaS) auf einem Server betrieben, handelt es sich dabei nicht um eine Weitergabe an Dritte. Nur bei solchen Weitergaben aber verlangt die GPL, dass das GPL-lizenzierte Stück Software jedem Interessierten im Quellcode zur Verfügung gestellt werden muss. Beim reinen Server-Einsatz könnte man GPL-Weiterentwicklungen daher von der Open-Source-Community fernhalten.

Möchte ein Programmentwickler erreichen, dass seine Programme auch in solchen Fällen jedem im Quellcode zur Verfügung stehen, sollte er die Affero GPL v3 wählen. In Abschnitt 13 schreibt sie nämlich vor, dass unter der AGPLv3 lizenzierte Programme allen Nutzern in der jeweils aktuellen Fassung im Quellcode als Download zur Verfügung stehen müssen. Als weitere Besonderheit regelt sie, dass ein Verlinken eines AGPLv3-Programms mit einem GPLv3-lizenzierten Programm zulässig ist und – das ist die Besonderheit – in einem solchen Fall aber das verlinkte Programm nicht unter die AGPLv3-Lizenz fällt, sondern weiterhin unter der GPLv3-Lizenz steht.

Tobias Haar

Urteil des EU-Gerichtshofes bringt Bewegung

Nachdem Microsoft Ende 2007 mit seiner Klage gegen das von der EU-Kommission im Rahmen des Kartellverfahrens verhängte Bußgeld gescheitert ist, gingen Open-Source-Enthusiasten aus dem Samba-Umfeld in die Offensive und forderten Microsoft in einem offenen Brief auf, die in den Auflagen festgelegten Informationen über die Kommunikationsprotokolle zwischen Windows-Servern und deren Schnittstellen herauszugeben.

Inzwischen hat man sich mit dem Redmonder Hersteller auf eine Regelung geeinigt, die sich Interessenten unter samba.org/samba/PFIF/PFIF_agreement.{html|pdf} ansehen können. Die eigens vom Software Freedom Law Center (SFLC, www.softwarefreedom.org) gegründete Protocol Freedom Information Foundation (PFIF, www.protocolfreedom.org) zahlt Microsoft einmalig eine Gebühr von 10 000 Euro. Dafür darf sie Open-Source-Programmierern Zugriff auf die Microsoft-Dokumentation einräumen. Die Entwickler dürfen diese Informationen grundsätzlich frei nutzen und müssen sich lediglich verpflichten, die Dokumentation selbst nicht weiterzugeben. Der mit deren Hilfe entstandene Code unterliegt keinen Einschränkungen, sieht man einmal vom leidigen Thema Patente ab: Die Regelung schließt die Nutzung eventuell betroffener Patente aus. Microsoft ist aber verpflichtet, eine Liste von ihrer Meinung nach betroffenen Patenten bereitzustellen, sodass die Entwickler sich darauf einstellen können.

Falsche Fehlermeldung: Kaufrücktritt

Mit einem Fehler, der nach Meinung des Verkäufers keiner war, hatte sich das OLG Koblenz zu befassen. Der Käufer eines komplexen EDV-Systems war vom Kaufvertrag zurückgetreten, weil nach den Backup-Läufen regelmäßig eine Fehlermeldung erschienen war und er davon ausgehen musste, dass die Datensicherung nicht erfolgreich abgeschlossen werden konnte. Bei der aufwendigen und zeitintensiven „Fehlersuche“ stellte sich aber jedes Mal heraus, dass kein Fehler vorlag, sondern die Meldung falsch war. Die Richter waren der Meinung, dass es dem Käufer eines solchen EDV-Systems nicht zugemutet werden kann, ständig überprüfen zu müssen, ob wirklich ein Fehler vorliegt. Das genügte ihnen, um dem Käufer Recht zu geben. Er erhält nach Rückgabe der Anlage den Kaufpreis zurück. *Tobias Haar*

Leitfaden zur rechtssicheren Archivierung

Viele Unternehmen, die bereits die eine oder andere Form der elektronischen Archivierung einsetzen, bewahren derart erfasste Dokumente häufig unnötigerweise zusätzlich in Papierform auf. Darauf wies der Leiter der Abteilung Technologiepolitik im Bundeswirtschaftsministerium, Detlef Dauke, bei der Vorstellung der 32-seitigen Broschüre „Handlungsleitfaden zur Aufbewahrung elektronischer und elektronisch signierter Dokumente“ hin. Der Leitfaden beschreibt das Ergebnis eines TransiDoc-Projektes mit dem Titel „Anforderungen und Trends der langfristigen Aufbewahrung (Atla§)“, das im Jahr 2006 abgeschlossen wurde. Er gibt eine ausführliche Übersicht und Bewertung zu rechtlichen, branchen- und anwendungsspezifischen Erfordernissen elektronischer Archivierung.

Kernstück des Projektes waren die Definition und der Aufbau einer Referenzarchitektur, mittels derer Ausgangsdokumente einschließlich ihrer elektronischen Signatur nach festgelegten Regeln auf das Zieldokument transformiert und zusammen mit einem Bericht und einer neuen digitalen Signatur versiegelt werden können. Der Leitfaden (als PDF zu finden auf www.bmwi.de unter „Service“, „Publikationen“, „H“ für Handlungsleitfaden) dient Unternehmen als Orientierung, wenn sie vollständig und vor allem rechtssicher auf eine elektronische Archivierung umstellen. *Tobias Haar*

Unkonkrete Anpassungsklauseln in AGB sind unwirksam

Der Bundesgerichtshof hat eine Anpassungsklausel in den „Allgemeinen Geschäftsbedingungen“ (AGB) für unwirksam erklärt, die dem Verwender der AGB das Recht gab, für Vertragsabschlüsse bedeutende Einzelheiten einseitig ändern zu dürfen. Konkret ging es dabei um die folgende Klausel: „Die X AG (Verwender) behält sich das Recht vor, den Inhalt dieser AGB oder der jeweiligen LB/PL (= Leistungsbeschreibungen und Preislisten), Sondervereinbarungen und Online-Anzeigen anzupassen, soweit dies dem Kunden zumutbar ist.“ Insbesondere bemängelten die Richter, dass die Vertragspartner des Verkäufers aus der Regelung nicht entnehmen können, in welchen Bereichen sie mit Änderungen rechnen müssen. Das verstößt gegen das sogenannte Transparenzgebot des deutschen Rechts, wonach die AGB aus sich heraus verständlich sein müssen. Ist dies nicht der Fall, sind solche Klauseln unwirksam und der Verwender kann sich nicht auf ihre Geltung berufen. Darauf gestützte Anpassungen sind dann ebenfalls unwirksam. Gleiches gilt im Bereich der Preisanpassungsklauseln. Solche Zusätze sind im Bereich des Internetzugangs nur zulässig, wenn sie etwa von Kostenerhöhungen abhängen und der Provider die einzelnen Kostenelemente und ihre Gewichtung bei der Preiskalkulation offenlegt. *Tobias Haar*

Informationspflicht auch bei WAP-Angeboten

Mit einer der wenigen Rechtsstreitigkeiten im Zusammenhang mit der Nutzung der WAP-Technik hatte sich das Oberlandesgericht Frankfurt (Main) zu befassen. Die Richter stellten in ihrem Urteil fest, dass die gesetzliche Informationspflicht gegenüber privaten Verbrauchern im Bereich des Onlinevertriebs von Produkten auch beim Vertrieb via WAP-Zugriffe greift. Werden die erforderlichen Verbraucherinformationen aber mittels einer externen Grafikdatei angezeigt, genügt das nicht, wenn eine Anzeige der Informationen aus technischen Gründen unterbleibt. So auch bei der WAP-Nutzung von Ebay, die Gegenstand der Klage war. Denn der Nutzer, der auf diesem Weg auf die Webseiten des Anbieters zugreift, bekommt diese externen Dateien nicht zu sehen. Damit verletzt der Verkäufer aber seine Informationspflicht.

Als Folge kann der Käufer – weil er über seine Rechte nicht ordentlich informiert wurde – auch noch nach Ablauf der eigentlichen Rücktrittsfrist den Kaufvertrag rückgängig machen und vom Verkäufer die Rückzahlung des Kaufpreises verlangen. Daneben droht ein Vorgehen durch Konkurrenten, die Unterlassung und Schadensersatz verlangen könnten. *Tobias Haar*

Urteil zur Haftung von Zugangsprovidern

Die juristischen Auseinandersetzungen um die Verantwortlichkeit der Zugangsprovider (Access-Provider) für über das Internet verbreitete Inhalte nehmen wieder einmal zu. Derzeit geht es vor allem um den Zugriff auf pornografische Seiten. Internet Service Provider (ISP) haften nach EU-Recht – das in dieser Form auch in Deutschland gilt und im Telemediengesetz geregelt ist – nur eingeschränkt. Denn sie sind als reine Telekommunikationsanbieter zu verstehen, die nur den Zugang zum Internet schaffen, selbst aber keinen Einfluss auf die dort abrufbaren Inhalte haben. So sahen es auch die Richter des Landgerichts Frankfurt (Main). Der dort verklagte ISP wurde daher nicht dazu verurteilt, den Zugriff auf bestimmte möglicherweise rechtswidrige Seiten zu verhindern. Ein wesentlicher Grund war nach Ansicht der Richter auch die für den ISP nicht ersichtliche „zurechenbare Ursache für eine Verletzung von Rechten des Anspruchstellers“. Außerdem fehlt ihm in der Regel mangels vertraglicher Beziehungen zum Webseitenanbieter eine rechtliche Grundlage, um auf die Verhinderung der Einstellung rechtswidriger Inhalte in das Internet hinzuwirken. *Tobias Haar*

Oft zu beanstandende Formulierung

Das Landgericht Hamburg hatte über die Klage eines Wettbewerbers gegen seinen Konkurrenten zu entscheiden. Dieser hatte auf seiner Webseite angegeben, „kein offizieller Vertragspartner“ eines anderen bekannten Produzenten zu sein. Gegen dieses unübliche Gebaren war der Kläger mit der Begründung vorgegangen, dies sei wettbewerbswidrig und diene nur dem Zweck, Kunden des genannten Produzenten auf das eigene Warenangebot umzuleiten.

Gerade wenn durch solche Namensnennungen auch die Webseiten von Konkurrenten in Internet-Suchmaschinen gelistet werden, droht juristischer Ärger. Im konkreten Fall waren die Richter aber der Meinung, dass im Bereich der Herstellung und des Vertriebs von sogenannten Hubwagen Kundenkontakte in der Regel nicht über das Internet erfolgen. Deswegen war der Negativ-Hinweis der Beklagten, kein Vertragspartner eines anderen bekannten Herstellers von Hubwagen zu sein, rechtlich nicht zu beanstanden. Die Richter machten aber deutlich, dass es sich hier um eine Entscheidung handelte, die sie so nur wegen der besonderen Umstände des Falles fällen konnten. *Tobias Haar*

Neuer Weg zur Dissertation

Die internationale Graduiertenschule für Informatik in Saarbrücken, die Fördermittel im Rahmen der Exzellenzinitiative der Bundesregierung erhält, bietet künftig die gesamte Doktorandenausbildung in der Informatik an der Universität des Saarlandes. Die Struktur des Studien- und Promotionsmodells orientiert sich stark am US-amerikanischen Vorbild.

So können interessierte Studierende ohne den Umweg über den Masterabschluss direkt in das Doktorandenprogramm einsteigen. Sie werden im Anschluss an das Bachelor-Studium in drei Semestern mit Vorlesungen und Seminaren in wissenschaftlicher Breite ausgebildet. Danach steht eine Qualifizierungsprüfung an, der die Forschungs- und Dissertationsphase folgt. Alternativ können wie bisher Studierende nach dem Masterabschluss in die Forschungsphase aufgenommen werden und vor der Dissertationsphase eine Qualifizierungsprüfung ablegen.

Eine finanzielle Unterstützung ist nach offiziellen Angaben garantiert. An Forschung und Lehre im Rahmen der Graduiertenschule beteiligen sich neben der Informatik an der Uni des Saarlandes das Max-Planck-Institut für Informatik, das Max-Planck-Institut für Softwaretechnik sowie das Deutsche Forschungszentrum für KI.

Mehr Studierende im Fach Informatik

Nach dem deutlichen Rückgang Anfang des Jahrzehnts und einer mehrjährigen Stagnation auf niedrigem Niveau steigen die Neuimmatrikulationen in der Informatik wieder; im Wintersemester 2007/2008 waren es knapp über 30 000. Im vergangenen Jahr schrieben sich dagegen gerade einmal 29 000 Personen neu für ein Informatikstudium ein. Das teilte das Statistische Bundesamt mit.

Da die Zahl der Neueinschreibungen für alle Fächer um rund 4 % wuchs, lässt sich der nun registrierte leichte Anstieg kaum als ein neu aufloderndes Interesse an der Informatik interpretieren. Trotz hervorragender Berufschancen ist die Studienanfängerzahl in der Elektro- und Informationstechnik ebenso ernüchternd. Nachdem die Anfängerzahl an den Unis im Vorjahr um 4 % sank, stagnierte sie nach Angaben des Fachverbandes VDE 2007 bei rund 7800 Neueinschreibungen.

KURZ NOTIERT



Eingebunden: Die Cisco Networking Academy hat für ihre Website gemeinsam mit Stepstone ein Stellenportal kreiert. Auf www.netacadadvantage.com können nun die 465 000 Studenten und Absolventen der Akademie in Europa, Afrika und dem mittleren Osten die Jobangebote in ihrem speziellen Aufgabengebiet einsehen.

Headhunting: Eine digitale Variante des Headhunting stellt das Recruiting-Portal www.jobleads.de vor. Die Vermittlung von Fach- und Führungskräften für offene Positionen erfolgt quasi auf Empfehlung. Registrierte „Talent Scouts“ sollen hierzu innerhalb ihres eigenen Bekanntenkreises geeignete Personen auf die offene Stelle aufmerksam machen.

Rückgang: In der hiesigen Wirtschaft gibt es laut Bitkom derzeit 43 000 offene Stellen für IT-Fachleute. Davon entfallen 18 000 auf die IT-Branche und 25 000 auf andere Wirtschaftszweige. Das führte dazu, dass die Zahl der bei der BA gemeldeten arbeitslosen IT-Spezialisten im November erstmals seit zwei Jahren unter die 30 000er-Marke sank.

Neue Eigner: Der niederländische Personaldienstleister Vedior NV übernimmt 70 % der Gesellschaftsanteile der Münchner Gulp, Betreiber des gleichnamigen IT-Projektportals. Vedior selbst steht wiederum vor der Übernahme durch Randstad.

KURZ NOTIERT

Cebit-los: Den Wegfall der Halle 1 nutzten D.velop, Easy Software und Windream dafür, ihre Teilnahme an der Cebit abzusagen. Als Grund nannten die Spezialisten für Dokumentenmanagementsoftware (DMS) unter anderem die Verlegung der DMS-Area von Halle 1 in Halle 3 sowie die Verlegung der Messezeit auf Dienstag bis Sonntag.

Vom Tisch: Die Pläne zur Aufspaltung des Internet- und Mobilfunk-Providers Freenet.de sind erst einmal begraben. Jetzt beabsichtigt das Management eine Holding-Struktur einzuführen, bei der das DSL- und das Portalgeschäft in eigenen Tochtergesellschaften geführt werden sollen.

Nomen est omen: SWsoft benennt sich in Parallels um. Schließlich ist das gleichnamige Virtualisierungsprodukt ungleich bekannter als der bisherige Firmenname des Herstellers. Mit dem Kauf der britischen Webhost Automation hat man zudem das Produktportfolio um eine umfassende Management- und Abrechnungslösung für gehostete Windows-Server ergänzt.

Ausstieg: Combots, die Nachfolgefirma von Web.de, stellt die fast 400 Mio. € schwere Beteiligung an United Internet zum Verkauf. Die Aktien, die man im Zuge des Verkaufs von Web.de an United Internet erhielt, werden nach Angaben des Managements allein noch als reines Investment und nicht mehr als strategische Beteiligung behandelt.

Neue Eigner: Der niederländische Personaldienstleister Vedior NV übernimmt 70 % der Gesellschaftsanteile der Münchner Gulp, Betreiber des gleichnamigen IT-Projektportals. Vedior selbst steht wiederum vor der Übernahme durch Randstad.

100-Milliarden-Dollar-Umsatzgrenze übertroffen

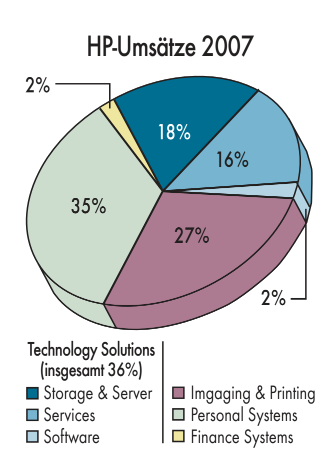
HP: Das neue Blau

Achim Born

Als erstes IT-Unternehmen überhaupt konnte HP einen Jahresumsatz von mehr als 100 Mrd. $ erwirtschaften. Und die Aussichten bleiben erfreulich, denn für die kommenden Geschäftsjahre verspricht das Management eine Verbesserung der Gewinnmarge bei allerdings geringerem Wachstum.

Seit einigen Quartalen führen die Statistiken einschlägiger Marktbeobachter Hewlett-Packard als Nummer 1 unter den PC-Herstellern. Dank des gut laufenden PC-Geschäftes im Schlussquartal des im Oktober beendeten Geschäftsjahres 2007 legte der US-Konzern eine erfreuliche Bilanz vor.

Der Quartalsumsatz kletterte um 14 % auf 28,3 Mrd. $, der Nettogewinn steigerte sich ebenfalls zweistellig auf 2,2 Mrd. $. Mehr als ein Drittel des Umsatzes im vierten Quartal steuerten die Einnahmen der PC-Gruppe (PC, Notebooks und Workstation) bei, die im Jahresvergleich um 30 % hochschnellten. Die zweitgrößte Sparte, das traditionell starke Geschäft mit Bildverarbeitung und Druckern (Imaging & Printing Group), wuchs um vergleichsweise bescheidene 4 % auf 7,6 Mrd. $. Es lieferte mit über 1 Mrd. $ jedoch das Gros des operativen Gewinns. Die Umsätze mit Servern und Speichersystemen legten um gut 10 % auf 5,2 Mrd. $ zu. Mit Services (Outsourcing etc.) wurden 4,4 Mrd. $ (+7 %) eingenommen. Den relativ größten Wachstumssprung machte der Software-Umsatz, der auf rund 700 Mio. $ verdoppelt wurde.



Die letztgenannten drei Geschäftssparten fasst HP neuerdings als Technology Solutions Group (TSG) zusammen. Im gesamten Geschäftsjahr stieg der Umsatz in dieser Sparte um 10 % auf 37,7 Mrd. $ und lag damit leicht über den Einnahmen der PC-Gruppe, die 36,4 Mrd. $ (+26 %) erwirtschaftete. Die Geschäfte der Imaging & Printing Group standen mit 28,5 Mrd. $ (+6 %) für 27 % der Geschäfte. Rund 2,3 Mrd. $ aus Finanzdiensten komplettierten die Konzerneinnahmen. Insgesamt stieg der Umsatz im Geschäftsjahr 2007 damit um 14 % auf über 104 Mrd. $, wobei ein Nettogewinn von 7,3 Mrd. $ unter dem Strich übrig blieb.

Zwei Punkte sind an der Bilanz beachtenswert: HP hat nun IBM endgültig als umsatzstärksten IT-Konzern abgelöst. Auch wenn der Vergleich ein wenig hinkt, da Big Blue keine PCs mehr produziert. In jedem Fall führten die von HP-Chef Mark Hurd eingeleiteten Umstrukturierungsmaßnahmen den Konzern nachhaltig in ruhigere Gewässer, nachdem die unter Carly Fiorina eingeleitete Fusion mit Compaq zunächst einige Turbulenzen ausgelöst hatte. Ungeachtet dessen besteht nach Ansicht des HP-Managements weiterhin die Notwendigkeit, an der Kostenschraube zu drehen. Vorgesehen ist unter anderem, durch Zusammenlegen von Standorten die Immobilienkosten bis 2010 um ein Drittel zu senken. Diese Maßnahmen sollen helfen, die operative Gewinnmarke von derzeit 9,2 % auf über 10 % anzuheben. Ein Ausbau der margenkräftigen Softwaresparte soll diesen Plan stützen. In Sachen Umsatz (für das Geschäftsjahr 2009 sind 117,1 bis 118,2 Mrd. $ vorgegeben) verfolgt man dagegen ein eher konservatives Ziel.

Die hiesige Hewlett-Packard GmbH erzielte im Geschäftsjahr 2007 im Übrigen einen Umsatz von 6,5 Mrd. €, was einem Plus von 10 % entspricht. Der Gewinn lag nach offizieller Verlautbarung im Bereich der Erwartungen. (WM)

Novell sieht rot – trotz der Kooperation mit Microsoft

Novell meldete leicht verspätet erst Mitte Dezember die Ergebnisse für das vierte Finanzquartal und Geschäftsjahr 2007 (endete am 31. Oktober). Im Schlussquartal verzeichnete das Unternehmen einen Umsatz von 245 Mio. $. Während die Einnahmen im Vergleich zum Vorjahresquartal leicht stiegen, blieb als Ergebnis der operativen Tätigkeit am Ende ein Verlust von 13 Mio. $ stehen. Deutlich verbessert wurden die Einnahmen mit Open-Platform-Produkten. Novell erzielte hier 23 Mio. $, wobei auf Linux Plattform-Produkte allein 22 Mio. $ (+69 %) entfielen. Statt eines kleinen Nettogewinns wie im Vorjahr stand in der Bilanz ein Nettoverlust von 44,4 Mio. $. Weit über ein Drittel der Einnahmen (355,6 Mio. $) erhielt man in Folge der Kooperation mit Microsoft. Das geht aus dem Jahresbericht an die Börsenaufsicht Securities and Exchange Commission (SEC) hervor.

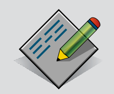
Neuerungen im ITK-Markt 2008

Im neuen Jahr müssen sich Verbraucher und Unternehmen auf eine Reihe gesetzlicher Änderungen einstellen. Bitkom stellte die in seinen Augen wichtigsten fünf Neuerungen zusammen. Dabei ist die Vorratsdatenspeicherung sicherlich die am heftigsten diskutierte. Ab Beginn dieses Jahres sind bekanntlich die TK-Anbieter verpflichtet, Verbindungsdaten aller Telefongespräche im Festnetz und im Mobilfunk sechs Monate lang zu speichern. Bevorratet werden nicht die Gespräche selbst, sondern Rufnummer, Dauer des Telefonats sowie die Standortdaten von Handys. Den Anbietern entstehen laut Verbandsangaben einmalige Kosten in Höhe von 75 Mio. € für den Aufbau der entsprechenden Infrastruktur sowie laufende Kosten im zweistelligen Millionenbereich pro Jahr. Ab 2009 folgen weitere Speicherpflichten für die E-Mail-Kommunikation, den Aufruf von Webseiten und die Internettelefonie. Die Kritik des Bitkom gegen die Vorratsdatenspeicherung richtet sich vornehmlich gegen die als zu gering erachteten Entschädigungsgelder für den technischen Aufwand. In der Öffentlichkeit dagegen wird über die grundsätzliche Verfassungsmäßigkeit des Gesetzes diskutiert; rund 30 000 Personen haben beim Bundesverfassungsgericht in Karlsruhe eine Klage eingereicht.

Zu weiteren Neuerungen, die Bitkom auflistet, zählen das neue Urheberrecht und die Unternehmensteuerreform. Ein Schwerpunkt ist die Novellierung des Abgabensystems für Aufzeichnungsgeräte wie DVD-Rekorder und ihre Speichermedien. Auf den ersten Blick positiv ist laut dem Interessenverband die Unternehmensteuerreform, mit der die Steuersätze für Unternehmen von durchschnittlich 38,6 % auf 29,8 % reduziert werden. Allerdings werden die geringeren Steuersätze mit einer Verbreiterung der steuerlichen Bemessungsgrundlage erkauft. Die ITK-Industrie trifft vor allem die Senkung der Betragsgrenze für die Sofortabschreibung geringwertiger Wirtschaftsgüter auf 150 € und die anteilige Hinzurechnung von Lizenzgebühren (z. B. für Software) bei der Gewerbesteuer.

Wenig glücklich ist Bitkom zudem mit den sogenannten Mobilfunkblockern, die seit diesem Jahr in mehreren Bundesländern unerlaubte Handygespräche in Gefängnissen unterbinden sollen. Wohl zu Recht befürchtet der Lobbyverband, dass das von den Blockern produzierte künstliche Funkloch den Mobilfunkverkehr außerhalb des Gefängnisareals beeinträchtigt.

KURZ NOTIERT



Optimistisch: Die deutsche ITK-Industrie blickt weiterhin mit großer Zuversicht in die Zukunft. 78 % der Unternehmen erwarten im neuen Jahr steigende Umsätze. 16 % rechnen mit einem stabilen Geschäft und nur 6 % gehen von sinkenden Umsätzen aus. Das geht aus einer aktuellen Umfrage des Lobby-Verbandes Bitkom hervor.

Im Plus: Progress erzielte im vierten Quartal einen Umsatz von 137 Mio. $. Das sind 12 % mehr als im entsprechenden Vorjahresquartal. Der Gewinn auf GAAP-Basis kletterte um 66 % auf 15,8 Mio. $. Im gesamten Geschäftsjahr 2007 stiegen der Umsatz um 10 % auf 494 Mio. $ und der Gewinn um 40 % auf 57,2 Mio. $.

Eingekauft: Die Einkaufstour der IBM setzt sich 2008 fort. Zum Jahresbeginn übernahm Big Blue den israelischen Speicherspezialisten XIV. Die finanziellen Details der Akquisition wurden nicht veröffentlicht.

Ausgebaut: Speicherspezialist Netapp baut die Managementsoftware-Sparte aus. Mit der Übernahme der nicht börsennotierten Onario erhält das Unternehmen Zugriff auf Softwarelösungen zur Automatisierung von Speichernetzen.

Halbleitermarkt mit Umsatzplus

Im vergangenen Jahr legten die Einnahmen im Halbleiter-Markt weltweit laut der von Gartner regelmäßig durchgeführten Markterhebung um 2,9 % zu. Laut dem vorläufigen Zahlenwerk ist das Volumen auf 270,3 Mrd. $ gestiegen. Dabei konnte Marktführer Intel aufgrund eines überdurchschnittlichen Wachstums von 8,2 % den Marktanteil auf 12,2 % (2006: 11,6 %) ausbauen. Wie im Vorjahr bekleidete Samsung Platz Zwei. Neue Nummer Drei unter den führenden Herstellern war im vergangenen Jahr Toshiba. Das japanische Unternehmen steigerte bei einem Umsatzzuwachs von knapp 28 % den eigenen Marktanteil auf 4,6 %. Texas Instruments, 2006 noch auf diesem Rang, rutschte bei einem Umsatzminus von 4,2 % um einen Platz in der Liste nach unten.

Das gleiche Schicksal ereilte Infineon (einschließlich Qimonda). Das Münchener Unternehmen musste 2007 unter den führenden zehn Anbietern mit 6,8 % den höchsten Umsatzrückgang hinnehmen.

Die Top Ten im Halbleitermarkt

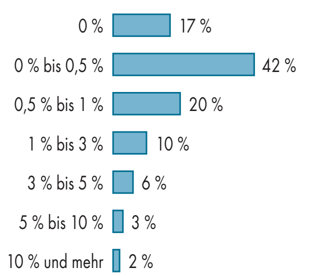
Rang 2007	Rang 2006	Firma	Umsatz 2007	Marktanteil	Umsatz 2006	Marktanteil
1	1	Intel	32,9	12,2	30,4	11,6
2	2	Samsung	20,9	7,7	20,1	7,7
3	6	Toshiba	12,5	4,6	9,8	3,7
4	3	Texas Instrument	11,5	4,2	12,0	4,6
5	5	STM	9,9	3,7	9,9	3,7
6	4	Infineon	9,8	3,6	10,5	4,0
7	7	Hynix	9,6	3,6	8,0	3,0
8	8	Renesas	8,0	3,0	7,9	3,0
9	11	NXP	5,8	2,2	5,9	2,2
10	12	NEC	5,8	2,1	5,7	2,2
		andere	143,5	52,7	142,5	54,2
		gesamt	270,3	100,0	262,7	100,0

Umsatzzahlen in Milliarden Dollar, Marktanteile in Prozent

Tücken des Internet-Verkaufs

Die Zahlungsmoral lässt auch im elektronischen Handel zu wünschen übrig. Zu diesem Schluss gelangt eine von Ibi Research im Auftrag der Wirecard AG durchgeführten Onlinebefragung. Danach müssen 11 % der Unternehmen Umsätze in Höhe von 3 % und mehr abschreiben, während 59 % der Unternehmen keine oder nur geringe (weniger als 0,5 % des Umsatzes) Zahlungsausfälle verbuchen. 30 % der Unternehmen nehmen Zahlungsausfälle zwischen 0,5 % und 3 % des Umsatzes hin. Über 40 % der Unternehmen gaben laut Umfrage an, dass mehr als 3 % der ausstehenden Rechnungen nicht rechtzeitig beglichen wurden. Der Anteil der nicht eingelösten oder zurückgebuchten Lastschriften beträgt bei 23 % der Unternehmen mehr als 3 % der per Lastschrift bezahlten Umsätze. Im Durchschnitt über alle Zahlungsverfahren liegt der Anteil der Zahlungsstörungen an den Internet-Umsätzen bei jedem fünften Unternehmen über 3 %. Jeweils etwa die Hälfte der Unternehmen ist der Ansicht, die Häufigkeit von Zahlungsstörungen und Zahlungsausfällen hätten in den vergangenen beiden Jahren zugenommen oder würden in den kommenden beiden Jahren weiter zunehmen. Nur etwa zehn Prozent der Unternehmen erwarten eine bessere Zahlungsmoral.

Umsatzausfälle bei Internet-Verkäufen





Googles mobile Plattform Android

Komplettpaket

Markus Stäuble

Fast gleichzeitig mit Apples iPhone erschien Android: Eine freie Java-Plattform für mobile Endgeräte auf einem Linux-Unterbau. Sie soll die Betriebssystemkonkurrenz das Fürchten lehren. Ein erster Blick auf die Pre-Release zeigt, was dran und drin ist.

Java auf dem Smartphone war bisher immer ein Synonym für JavaME mit einer lizenzierten Laufzeitumgebung von Sun Microsystems. Nun schickt Google zusammen mit über 30 Partnern Android ins Rennen – eine Plattform, die diese Gleichung ins Wanken bringt. Ungewöhnlich an ihr ist vor allem, dass am Ende einer in Java entwickelten Anwendung kein herkömmlicher Bytecode steht.

Apple hat mit der Veröffentlichung seines iPhone einiges an Unruhe in den Markt der mobilen Endgeräte gebracht. Google reagierte Anfang November 2007 darauf mit der Veröffentlichung seiner eigenen Softwareplattform. Um ihr eine gehörige Mitgift zu geben, hat Google so nebenbei mit anderen (unter anderem T-Mobile, Telecom Italia, Motorala, Samsung, Intel) die Open Handset Alliance (www.openhandsetalliance.com) gegründet. Besonders interessant an dieser Konstellation ist die Lizenzpolitik der veröffentlichten Plattform. Anders als andere Betriebssysteme von Mobilfunkgeräten wird Android in der endgültigen Fassung unter der Apache-Lizenz (v2) veröffentlicht werden.

Bis zu 10 Millionen für Entwickler

Nach aktuellem Stand soll die Plattform im zweiten Halbjahr 2008 in einer stabilen Fassung erscheinen. Zu diesem Zeitpunkt will der Gerätehersteller HTC ein erstes Handy mit Android auf den Markt bringen. Um zum Start bereits einige Anwendungen (vielleicht sogar schon die lang erwartete Killerapplikation) anbieten zu können, hat Google Android vorab veröffentlicht und aktualisiert es kontinuierlich. Ein mit 10 Millionen US-Dollar dotierter Wettbewerb soll Entwickler für die Plattform gewinnen (code.google.com/android/adc.html, Einreichungen sind bis einschließlich 3. 3. 2008 möglich).

Ein Blick auf die Android-Architektur zeigt, was diese Plattform von anderen für mobile Endgeräte unterscheidet. Ihre Basis bildet ein Linux-Kernel der Version 2.6. Er ist für grundlegende Dinge wie Speichermanagement, Netz und Treiber zuständig. Java fungiert als Implementierungssprache für Anwendungen. Als Compiler der Java-Klassen arbeitet nur der im JDK5 oder 6 enthaltene, das Gnu-Produkt funktioniert nicht. Dem Übersetzen in Java-Bytecode folgt das Erstellen eines „Dalvik Executable“ mit der Endung *.dex*. Dafür ist das im *tools*-Verzeichnis mitgelieferte Programm *dx* zuständig.

Das so erzeugte Executable läuft innerhalb der Dalvik VM. Mit anderen Worten: Das endgültige Kompilat ist nicht kompatibel zum klassischen Bytecode von Java. Dadurch fallen keine Lizenzkosten an – anders als bei einer VM von Sun. Technisch gesehen provoziert dieses Konzept eine Spaltung von Java, denn die Entwicklung ging völlig am JCP (Java Community Process) vorbei. Es ist unter anderem nicht auszuschließen, dass Android bei hinreichendem Erfolg Sprachmittel aufnimmt, die nicht mehr kompatibel zum „anderen“ Java sind. Einige Bibliotheken, etwa die relationale Datenbank SQLite, komplettieren Android. Die entwickelten Applikationen können auf ein mitgeliefertes Framework zurückgreifen.

Arbeiten auf drei Betriebssystemen

Erster Schritt für die Installation des Android SDK ist das Herunterladen von code.google.com/android/download.html. Die Entwicklungsplattform steht für Windows XP oder Vista, Mac OS X 10.4.8 oder höher und Linux zur Verfügung. Für jedes Betriebssystem gibt es ein knapp 60 MByte großes ZIP-Archiv, das man nur in das gewünschte Verzeichnis entpackt.

Dort befinden sich neben dem Archiv *android.jar* drei Verzeichnisse: *docs* (Dokumentation), *samples* (Beispiele) und *tools* (Hilfsprogramme und Bibliotheken). Einer der wichtigsten Android-Bestandteile neben der API (in *android.jar*) ist der Emulator im Verzeichnis *tools* (unter Windows als *emulator.exe* startbar), in dem sich die

entwickelten Anwendungen testen lassen. Zwar ist es möglich, nur mit dem SDK eine Anwendung für Android zu entwickeln und sie im mitgelieferten Emulator zu testen. Einfacher und schneller geht es jedoch mit Eclipse 3.3 und dem dafür entwickelten Android-Plug-in. Seine Installation lässt sich am einfachsten über den Update-Manager von Eclipse bewerkstelligen. Hierzu ist zunächst in Eclipse über „Help | Software Updates | Find and Install“ der Update-Manager zu öffnen. Nach dem Auswählen von „Search for new features to install“ im ersten Dialog trägt man als „New Remote Site“ *https://dl-ssl.google.com/android/eclipse/* ein. „Finish“ startet die Suche nach der neuesten Version, die ein Klick auf „Next“ schließlich installiert. Nach dem anschließenden Neustart von Eclipse führt „Windows | Preferences | Android“ zum Konfigurationsdialog des Plug-in. Dort muss man zumindest den Pfad zum Android SDK eintragen.

Listing 1: Auszug aus der GUI-Definition

```
<TableLayout
 xmlns:android="http://schemas.android.com/apk/res/android"
 android:layout_width="fill_parent"
 android:layout_height="wrap_content"
 android:padding="10px"
>
<TextView id="@+id/result"
     android:layout_width="fill_parent"
     android:layout_span="6"
     android:background="@android:drawable/editbox_background"
 />

<Button id="@+id/button7"
          android:layout_width="wrap_content"
          android:layout_height="wrap_content"
          android:layout_alignParentRight="true"
          android:layout_marginLeft="10px"
          android:text="7" />
```

Listing 2: Auszug aus der Java-Implementierung

```
@Override
public void onCreate(Bundle icicle) {
..
setContentView(R.layout.calculator_layout);
textView = (TextView) findViewById(R.id.result);
// Add the listener for the buttons
Button button = (Button) findViewById(R.id.button0);
button.setOnClickListener(new InputButtonListener(0));
private class InputButtonListener implements
     OnClickListener {
       private int number;
     public InputButtonListener(final int number) {
     this.number = number;
   }
...
    public void onClick(final View view) {
// Initialize the number storage.
     if (theNumber == null) {
     theNumber = new StringBuffer("");
   }
  // append the digit
     theNumber.append(number);
/*
 * If last operation equals reset the text field.
 */
if (lastOpEquals) {
     textView.setText("" + number);
     lastOpEquals = false;
} else {
     textView.append("" + number);
}
```

Ein kleines Beispielprojekt soll einen ersten Eindruck von der Anwendungsentwicklung mit dem SDK vermitteln. Da die Dokumention von Android bereits ein Tutorial für ein typisches Hello World enthält, soll dies nicht als Anschauungsobjekt dienen – stattdessen ein simpler Taschenrechner mit den Operationen Plus und Minus. Zur Entwicklung diente das Eclipse-Plug-in unter Windows. Der erste Schritt ist das Anlegen eines Android-Projekts via „File | New | Android Project“. Im anschließenden Dialog sind neben dem Projektnamen die Bezeichnungen für Package, Activity und Application einzutragen.

Taschenrechner statt Begrüßung

Der Name des Projekts entspricht dem des Verzeichnisses, das die Projektdateien enthält. Der Package-Name ist vergleichbar mit den von Java her bekannten Packages: Unter dem angegebenen Paket liegen die Quellen für die Anwendung. Begrifflich neu ist der „Activity Name“. Im Android-Umfeld bezeichnet er eine lauffähige Einheit, also die Startklasse der Anwendung. Das Plug-in generiert daraus eine von *android.app* abgeleitete Klasse des angegebenen Namens. Der Application Name benennt die Anwendung und erscheint als Titel im jeweiligen Endgerät.

Nach dem Ausfüllen des Wizard öffnet sich das Projekt. Die generierte Activity enthält einige Zeilen Quellcode, die der Entwickler im Laufe seiner Arbeit anpasst. Neben dem Verzeichnis mit den Quellen gibt es *assets* und *res*. Letzteres versammelt die nötigen Ressourcen in den Unterordnern *drawable* für Grafiken, *layout* für die Beschreibung der Oberfläche und *values* für Wertdefinitionen, zum Beispiel Beschriftungen.

R ist immer gut informiert

Für das Beispielprojekt bietet sich „Calculator“ als Projektname an. Seine Oberfläche kann man sowohl im Quellcode als auch in einem XML-Dialekt beschreiben. Da es unter Umständen viel Arbeit erfordert, ein GUI direkt im Javacode zu erstellen, kam hier die XML-Variante zum Zug. Nach dem Erzeugen des Projekts existiert in *res/layout* bereits die Datei *main.xml*, die zur besseren Kennzeichnung den Namen *calculator_layout.xml* bekommt (s. Listing 1).



Im Android-Emulator lassen sich die Anwendungen ausprobieren. In Verbindung mit dem Eclipse-Debugger dient er zur Fehlersuche (Abb. 1).

Als Tasten des Taschenrechners fungieren *Button*-Komponenten. Zur Anordnung von Elementen stellt die Android-API einige Layouts zur Verfügung; der Taschenrechner benutzt das *TableLayout*. Für die Anzeige des Ergebnisses verwendet er die Komponente *TextView*. Erwähnenswert in diesem Zusammenhang: Grafiken aus dem Verzeichnis *res/drawable* lassen sich über *@android:drawable/bildname_ohne_endung* verwenden (zum Beispiel als Hintergrund).

Außer der generierten Activity existiert eine Datei *R.java* im selben Paket, die das Plug-in im Hintergrund bei Änderungen im Verzeichnis *res* aktualisiert. Diese Klasse bietet Zugriff auf die einzelnen Elemente der Oberfläche. Dazu haben alle im XML-Layout verwendeten Komponenten einen

eindeutigen Bezeichner (*id*). Als Letztes bleibt noch die Implementierung der Logik und ihre Verbindung zur Oberfläche. Wie in Java üblich, reagieren *Listener* auf Aktionen innerhalb des GUI. Für jeden Button ist ein *android.view.View.OnClickListener* zuständig (s. Listing 2). Analog gibt es Listener für die Operationen Plus und Minus sowie den „=“-Button. Jeder kann über die ID die Ergebniszeile (*TextView*) suchen und ihren Text geeignet setzen. Zu guter Letzt darf man nicht vergessen, das erzeugte Layout hinzuzufügen, wozu man es wiederum über die Klasse *R* ansprechen kann:

```
setContentView(R.layout.calculator_layout);
```

Einem Test der Anwendung steht jetzt nichts mehr im Wege. Für ihren Start ist eine via „Run | Open Run Dialog … | Android Application“ erzeugte Run-Konfiguration erforderlich, für die der Entwickler das Projekt und die Activity auswählt. Er startet zunächst per Run-Konfiguration die Activity, dann den Emulator, der als Erstes Android bootet. Danach führt der Emulator die zuvor konfigurierte Activity aus.

Er erscheint in Gestalt eines Smartphone (s. Abb. 1). In der Run-Konfiguration lässt sich mit dem Reiter „Emulator“ unter anderem die Bildschirmgröße des Smartphones wählen. Für das in Abbildung 1 dargestellte Smartphone wurde die Größe HVGA-P verwendet.

Nach dem Booten lädt der Emulator die gestartete Anwendung und führt sie aus. Zur Fehlersuche kann man den Eclipse-Debugger verwenden. Dazu setzt man zunächst Haltepunkte an den gewünschten Stellen und startet dann das Programm im Debug-Modus, etwa per „Run | Debug History | Calculator“.

Fazit

Durch die Entwicklung einer Anwendung mit und für Android bekommt man ein erstes Gefühl von der Leistungsfähigkeit dieser Plattform. Die Open Handset Alliance hat mit großem Anschub von Google die richtigen Zutaten ausgewählt, die Entwickler und Anbieter an den Tisch locken. Vor allem die Verwendung von Java öffnet diese Plattform für viele Firmen und Entwickler.

Stärkstes Argument für Android ist aber nicht die Sprache, sondern die Kombination von Linux mit einer eigens dafür entwickelten VM. Das ermöglicht es, die Plattform ohne Lizenzkosten auf mobilen Endgeräten anzubieten – ein großer Wettbewerbsvorteil. Der Preis dafür ist im Vergleich zu MIDP proprietärer Code. Dass zum Start der Plattform bereits eine große Armada von bekannten Firmen mitsegelt, lässt die Erwartungen weiter wachsen. Was die Konkurrenz bedrückt, kann die Endkunden nur freuen. Denn durch eine solche offene Plattform können viele Open-Source-Projekte für Android entstehen, und dies macht den Kauf eines damit ausgestatteten Endgerätes reizvoll. (ck)

MARKUS STÄUBLE

ist Senior Software Engineer bei namics (deutschland) GmbH. Schwerpunkte seiner Arbeit sind neben der Projektleitung und dem Coaching die Architektur von Java EE-Anwendungen sowie deren Qualitätssicherung.

Webanwendungen für das iPhone

Runde Ecken

Jochem Huhmann



Bislang können auf dem iPhone Anwendungen nur im Browser laufen. Wer seine Site für das Mobiltelefon anpassen will, muss manches beachten und kann auf allerlei Hilfsmittel zurückgreifen.

Lokale Applikationen durch im Browser laufende Webapplikationen zu ersetzen, gelingt sowohl auf Workstations als auch auf mobilen Geräten bisher nur eingeschränkt. Auf Apples iPhone (und dem bis auf den fehlenden Mobilfunkteil weitgehend identischen iPod touch) allerdings bleibt vorerst keine große Wahl, da ein SDK erst im Februar 2008 erscheinen soll. Ein Überblick über Features, Einschränkungen und Besonderheiten hilft bei der Entscheidung, ob und wie sich Webapplikationen für das Gerät optimieren lassen.

In Gegensatz zu den auf mobilen Geräten sonst meist anzutreffenden speziellen Produkten läuft auf dem iPhone Safari und damit ein weitgehend voll funktionsfähiger Browser. Er gaukelt dem Webserver eine Fensterbreite von 980 Pixeln vor und skaliert die Darstellung dann auf die vorhandenen 320 (bei horizontaler Orientierung 480) Pixel. Die meisten Seiten stellt er damit nahezu perfekt dar: Obwohl Fließtext so nur selten lesbar ist, kann man sich einen Überblick über Seiteninhalte und eingebettete Grafiken verschaffen und Überschriften lesen. Für Details zoomt Doppeltippen in einzelne Spalten und Blöcke hinein- und wieder heraus. Dabei bemüht sich Safari, die Elemente passgenau auf den Schirm zu bringen. Voraussetzung hierfür ist allerdings ein Seitenlayout, das den Textumbruch nicht vollständig dem Browser überlässt: Bei Zeilen, die sich über die gesamten (virtuellen) 980 Pixel erstrecken, bleibt einem nur die Wahl zwischen mikroskopisch winziger Darstellung oder kontinuierlichem horizontalen Scrollen nach freiem Hineinzoomen durch „Aufziehen“ eines Bereichs mit zwei Fingern. Webseiten, die die Textbreite nicht begrenzen, gibt es allerdings selten, da sie auf Desktops bei üblichen Fenstergrößen und Auflösungen leicht zu enormen Zeilenlängen führen und deshalb mittlerweile fast ganz ausgestorben sind.

Grenzen bei aufwendigem Layout

Für das reine Lesen von Webseiten ist diese Art der Darstellung und Bedienung auf dem kleinen Display überraschend gut geeignet. Sie stößt jedoch schnell an ihre Grenzen, wenn es um typische Webapplikationen geht: Großzügig horizontal und vertikal auf der Seite verteilte Eingabefelder, Buttons, Auswahllisten, Textkästen und dekorative Elemente erfordern viel Scrollen in alle Richtungen. Buttons sind oft so klein oder liegen so eng beieinander, dass sie sich in einer die Übersicht bewahrenden Zoomstufe nicht sicher treffen lassen. Zum Schluss darf man sich auf die Suche nach dem „Senden“-Button begeben. Kurz: Formulare sind eine Qual. Dass dies trotz der eingeschränkten Platzverhältnisse nicht so sein muss, beweisen die mitgelieferten und durchweg angenehm bedienbaren Anwendungen, die in der Regel noch nicht einmal besonders aufwendig gestaltet sind.

Webapplikationen lassen sich mit wenig Mühe für das iPhone optimieren. Will man den Nutzern „normaler“ Browser nicht eine sehr ungewohnte Ansicht bieten, wird man allerdings nicht um eine der (meist zu Recht) unbeliebten Browser-Weichen herumkommen. Mobile Safari auf dem iPhone beziehungsweise iPod touch meldet sich im *User-Agent*-Teil des HTTP-Header folgendermaßen:

```
Mozilla/5.0 (iPhone; U; ↵
  CPU like Mac OS X; en) AppleWebKit/420+ ↵
  (KHTML, like Gecko) ↵
  Version/3.0 Mobile/1A543 Safari/419.3
Mozilla/5.0 (iPod; U; ↵
  CPU like Mac OS X; en) AppleWebKit/420.1 ↵
  (KHTML, like Gecko) ↵
  Version/3.0 Mobile/3A101a Safari/419.3
```

Diesen Kopfzeilen sieht man auf den ersten Blick an, dass der mobile Safari gern als Webkit-, notfalls auch als Gecko-Browser (wie Mozilla/Firefox) oder als KHTML, aber auf gar keinen Fall als IE erkannt werden möchte. Will man ihn sicher als das identifizieren, was er ist, führt kein Weg an der Prüfung auf

„iPhone“ oder „iPod“ vorbei, zumal auch die Webkit-Versionen je nach OS-Version des Geräts variieren. Nebenher bemerkt legt die fehlende generische Identifikation wie „Mobile-Safari“ die Vermutung nahe, dass es in Zukunft noch weitere Geräte mit demselben Browser, aber mit anderen Fähigkeiten oder anderer Bildschirmauflösung geben könnte. Die bisherigen Versionen des iPhone und des iPod touch unterscheiden sich hinsichtlich der Fähigkeiten des eingebauten Browsers nicht.

Meta-Tags vermeiden Scrollen

Der erste Schritt besteht darin, horizontales Scrollen zu vermeiden. Die vom mobilen Safari angenommenen 980 Pixel Fensterbreite lassen sich mit dem *Viewport* Meta-Tag an die tatsächlichen Gegebenheiten anpassen. Im selben Schritt kann man das nun überflüssige Zoomen unterbinden:

```
<meta name="viewport"
  content="user-scalable=no, width=device-width">
```

Zum Ausblenden der beim expliziten Aufruf einer Webapplikation überflüssigen bis lästigen URL-Zeile reicht ein bisschen Javascript:

```
window.onload = function() {
  setTimeout(function(){window.scrollTo(0, 1);}, 100);
}
```

Es rollt den Bildschirminhalt um ein Pixel nach unten, wodurch Safari die URL-Zeile ausblendet und 60 Pixel mehr Platz schafft.

Bei derart optimierten Webapplikationen dürfte der Einstiegspunkt nach einem Titel und einem Logo am oberen Seitenrand ein Menü sein. Es sollte den mitgelieferten iPhone-Applikationen ähneln und eine einfache vertikale Auswahlliste von Textlinks anbieten. Schriftgröße und Zeilenhöhe müssen für das sichere Antippen mit dem Finger hinreichend groß gewählt sein: Apple empfiehlt 44 Pixel Zeilenhöhe und eine Schriftgröße von 14 Punkt, mit einem Pfeil am rechten Rand zur Verdeutlichung des Menücharakters. Damit lassen sich ungefähr fünf Einträge samt Überschrift und einer Fußzeile mit zwei bis drei Buttons (für Impressum, Registrierung et cetera) so unterbringen, dass sie ohne Scrollen sichtbar und mit einem Fingerdruck erreichbar sind.



Mit der Javascript-Bibliothek IUI lassen sich iPhone-Anwendungen mit wenig Aufwand erstellen (Abb. 1).

Weitere Inhalte (Neuigkeiten, Meldungen, Abkürzungen zu Inhalten) können weiter unten folgen. Dabei ist aber darauf zu achten, dass der mobile Safari Scrollbalken nur anzeigt, wenn der Benutzer den Inhalt tatsächlich verschiebt – es gibt keinen sichtbaren Hinweis darauf, dass die Seite größer ist als der gerade sichtbare Bereich. Deshalb sollten alle wichtigen Links im sichtbaren Bereich liegen. Im Vergleich zu manchen aufwendigen Startseiten mag all dies wie eine starke Einschränkung wirken, aber einen Vorteil hat die Konzentration: Der Einstieg ist übersichtlich und schnell sichtbar.

iX-TRACT

- Bislang können Anwendungen für das iPhone nur in dessen Safari-Browser laufen. Ein natives SDK soll es erst ab Februar 2008 geben.
- Webapplikationen sollten sich an den auf dem Gerät installierten Programmen orientieren. Entwickler können sich dazu bei Apple mit Grafiken bedienen und spezielle CSS-Attribute nutzen.
- Eine Debug-Konsole auf dem iPhone hilft bei der Fehlersuche in Webanwendungen. Auch die Firefox-Erweiterung Firebug lässt sich dazu nutzen.

Eine der wesentlichen Neuerungen im GUI von Nextstep und heute bei Mac OS X war die spaltenweise Navigation durch Hierarchien: Anstelle grafisch dargestellter Bäume und verzweigter Listen stellt der Finder in OS X Verzeichnishierarchien spaltenweise nebeneinander dar. Ein Klick auf eine Zeile (Verzeichnis) in einer Spalte öffnet eine neue rechts davon, die den Inhalt zeigt. Viele Menüs auf dem iPhone und iPod touch folgen dieser Konvention, und es gibt gute Gründe, dies bei Webapplikationen beizubehalten.

Menüs von Nextstep inspiriert

Im Unterschied zum Datei-Browser bei Nextstep und zum Finder bei Mac OS X hat das iPhone in der Regel nur Platz für eine Spalte auf dem Schirm. Umso wichtiger ist eine klare Navigation samt einfacher Rückkehr zur darüberliegenden Ebene. Dies erreicht meist ein pfeilartiger Button links in der obersten Zeile, der den Titel der letzten Ebene trägt und zu ihr zurückführt. Dieses Modell lässt sich einfach auf eine Hierarchie von Webseiten übertragen. Netterweise bietet Apple fertige Images samt CSS-Styles an (siehe Kasten „Onlinequellen“), die den üblichen GUI-Konventionen auf dem Gerät folgen. Zur Vermeidung unnötig übertragener Daten verwenden diese das proprietäre CSS-Attribut *-webkit-button-border*, das horizontal skalierende PNG-Grafiken auf beliebige Elemente stempelt. So lassen sich aus einer Grafik Buttons mit beliebigen Texten erzeugen, ohne für jeden Button eine weitere Datei übertragen zu müssen. Ähnliches gilt für die visuell leicht abweichenden Menüs für Einstellungsdialoge samt gerundeten Rahmen für gruppierte Einstellungen. Der „Senden“-Button, den man beim iPhone eher „Sichern“ oder „Fertig“ nennen sollte, ist übrigens auf Einstellungsseiten rechts oben am besten untergebracht.

Wem all dies nun zwar interessant, aber mühsam umzusetzen erscheint, der sei getröstet: Es existieren bereits Javascript-Bibliotheken wie IUI (s. Abb. 1), die dem Entwickler nicht nur den Großteil der Kleinarbeit abnimmt und fertige Hierarchien und Einstellungsdialoge zur Verfügung stellt, sondern auch Ajax-Techniken wie das Laden von Inhalten in die aktuelle Seite unterstützt. Open-Source-Applikationen wie das Mail-Programm *imobmail* sind eine nützliche Quelle zum Lernen und Experimentieren.

Eine der größten Schwächen von Webapplikationen nicht nur auf dem iPhone ist der eingeschränkte Zugriff auf Funktionen und Software des Betriebssystems. Im mobilen Safari aktiviert ein Klick auf „mailto“-URLs den integrierten Mailclient, „tel“-URLs rufen (nach Bestätigung des Benutzers) die angegebene Telefonnummer an, und bei Links auf Youtube-Videos oder Google-Maps benutzt das iPhone automatisch die eingebauten Clients. „sms“-URLs erkennt es nur in E-Mails, jedoch nicht auf Webseiten. Kontrolle über die bei Bedarf eingeblendete Tastatur gibt es nur begrenzt: Sprachspezifische Tastaturen lassen sich über das *lang*-Attribut des jeweiligen Eingabe-Feldes anfordern. Enthält der Feldname „zip“, bekommt man eine numerische Tastatur, bei „phone“ die Telefontastatur. Die von Safari im URL-Feld verwendete spezielle Tastatur lässt sich leider nicht programmatisch wählen.

Canvas statt Flash, SVG & Co.

Die Darstellung und Kontrolle komplexerer grafischer Elemente zum Beispiel für Charts oder virtuelle Geräte ist mangels Unterstützung für Flash, OpenGL, Java und SVG nur über das *Canvas*-Element möglich, das aber gut in Javascript und DOM eingebunden ist und auch in OS-X-Widgets Verwendung findet.

Fehler in Webapplikationen zu finden, ist aufgrund der Wechselwirkungen zwischen HTML, CSS, Javascript und serverseitig laufender Software oft eine Qual. Eine Plattform mit so vielen (notwendigen) Eigenheiten wie der mobile Safari erleichtert es dem derart geplagten Entwickler nicht, da bewährte Hilfen wie Firebug nur begrenzt einsetzbar sind.

Glücklicherweise hat Apple dem iPhone-Browser eine Debug-Konsole spendiert, die sich im Entwicklerabschnitt der Safari-Einstellungen aktivieren lässt. Safari blendet dann unterhalb der URL-Zeile eine Leiste mit der Anzahl der erkannten HTML-, CSS- und Javascript-Fehler ein, die nach Antippen in eine nützliche Fehlerliste mit Zeilennummern verzweigt. Buttons am unteren Rand erlauben es, nur HTML-, CSS- und Javascript-Fehler anzuzeigen. Auch Dinge wie die Laufzeitausgabe von Variablen sind damit möglich: die Zeile *console.log("var=" + var)* schreibt zum Beispiel den Namen und Inhalt der Variablen *var* in die Konsole. Außerdem gibt es *error()*-, *warn()*- und *info()*-Methoden, die die Ausgabe in der Konsole mit passenden Icons verzieren.

Als Steve Jobs dem ungläubigen Publikum verkündete, dass er sich bei Applikationen für das „Jesus Phone“ auf die Web-2.0-Idee verlässt, gab es nur wenige begeisterte Gesichter. Betrachtet man die Anzahl der Apple-eigenen Webseiten, die das iPhone berücksichtigen (bis auf minimale Anpassungen der Darstellung praktisch keine) und nimmt die kürzliche Ankündigung eines nativen SDK für Februar 2008 dazu, stellt sich die Frage: Wozu der Aufwand?

Der dünnste Thin Client als Ziel

Eine mögliche Antwort ist die etwas verblüffende Erkenntnis, dass Webapplikationen für das iPhone häufig trotz der vielen Einschränkungen besser benutzbar sind als ihre großen Vorbilder. Der Zwang zu hierarchischer Navigation und durchdachter Oberfläche sowie der geringe Spielraum für Layout-Unarten trotz Möglichkeiten für visuelle Finesse lassen erahnen, was Webapplikationen sein könnten, wenn man nur wollte. Deshalb sind sie auf dem iPhone zumindest nicht weniger sinnvoll als auf dem Desktop. Da der „Thin Client“ im Fall des iPod touch nur 8 Millimeter dünn ist, drängt sich der Schluss auf: Wenn schon Webapplikation, dann ist dies der richtige Client.

Während viele Entwickler bei Browser-Weichen und gerätespezifischen Entwicklungen aufstöhnen, könnte es gut sein, dass sie solche Anpassungen kaum mehr vermeiden können. Googles Android-Plattform für mobile Geräte verwendet dieselbe Browser-Basis, sodass die Zielgruppe für Webkit-Spezifisches sich bald nicht mehr auf iPhone- und Mac-Benutzer beschränken wird. So lief WPhone, eine iPhone-Anpassung für die Verwaltungsoberfläche des Blog-Systems Wordpress, nach nur geringen Änderungen auf Android.

Trotzdem, Apple muss nachbessern: Ein schwerwiegender Mangel des Geräts ist das Fehlen jeglicher Keychain-Unterstützung – Benutzernamen und Passwörter für Webseiten muss sich der Anwender merken und immer wieder von Hand eingeben. Wer einmal die vorhandenen Applikationen in Apples Verzeichnis durchprobiert, stellt schnell

fest, dass sogar eine simple Einkaufsliste eine Registrierung verlangt. Selbst wenn man (sicherheitstechnisch bedenklich) immer dasselbe Passwort benutzt, hört hier der Spaß schnell auf.

Abhilfe schafft bestenfalls OS-X-Shareware wie 1Password (1password.com) auf dem Mac zusammen mit einem Bookmarklet auf dem iPhone, aber nicht jeder hat einen Mac. Authentifizierung über IP-Adressen ist innerhalb kontrollierter Netze vielleicht ein Ausweg, in öffentlichen Netzen ist der Komfortverlust durch explizites Anmelden bei jeder Anwendung aber prohibitiv. Für weniger sicherheitsrelevante Angebote empfiehlt sich dringend das Speichern von Benutzerdaten in Cookies, wenn man die Anwender nicht vergraulen möchte. Dazu kommen Einschränkungen wie der fehlende Support für lokales Speichern von Daten und die daraus resultierende fehlende Unterstützung für Up- und Downloads sowie fehlendes Copy & Paste – beides ist zwar überraschend oft verzichtbar, aber wenn es fehlt, dann fehlt es richtig.

Unterm Strich ist der mobile Safari auf dem iPhone und iPod touch für viele Webapplikationen gut brauchbar. Diese Geräte können zwar größere Rechner genauso wenig ersetzen wie Webapplikationen alle nativen Programme. Trotzdem gibt es viele Fälle, in denen zentrales Vorhalten von Daten und Code zusammen mit einem leistungsfähigen mobilen Client den Aufwand der Anpassung lohnen. (ck)

JOCHEM HUHMANN

ist freiberuflicher Autor und Entwickler.

Onlinequellen

iPhone-Entwicklungszentrum
developer.apple.com/iphone/devcenter/

IUI
code.google.com/p/iui/

imobmail
www.andi.de/imobmail/

Webapplikationen
www.apple.com/webapps/

Firebug für iPhone
www.joehewitt.com/blog/firebug_for_iph.php

Beispiele für GUI-Techniken
groupaware.mobi/iphone/

iPhone-Entwicklung bei Google Groups
groups.google.com/group/iphonewebdev/



Sicherheitskonzepte von Symbian OS und Windows Mobile

Mal mit, mal ohne

Rayko Enz, Jörg Weber

Zwar lassen Handy-Viren nach wie vor auf sich warten, die beiden führenden Smartphone-Plattformen sind jedoch inzwischen gerüstet. Ein näherer Blick zeigt große Unterschiede bei den Sicherheitsmodellen und ihrer Umsetzung.

Zwei der wichtigsten mobilen Plattformen sind derzeit der Marktführer Symbian OS und Windows Mobile Version 6 von Microsoft. Dieser Artikel untersucht die Sicherheitsmerkmale der Betriebssysteme aus der Sicht eines Softwareentwicklers.



Symbian OS

Symbian OS, hergestellt und vertrieben von dem gleichnamigen Softwareunternehmen, ist mit etwa 70 % Anteil unter den Smartphones derzeit Marktführer dieses Segments. Der Hersteller entschloss sich Ende 2005, das Sicherheitskonzept für die Version 9.1 in ein mehrstufiges, mit Zertifikaten steuerbares Rechtesystem umzuwandeln. Im Detail besteht „Symbian Platform Security“ aus Capabilities, Signierung und Data-Caging.

Capabilities schützen als gefährdet eingestufte Funktionen des Systems. Dazu gehören APIs, deren Benutzung Kosten verursacht oder die Datenintegrität gefährdet. Diese APIs besitzen eine Capability. Ein Programm darf sie nur nutzen, wenn es mit einem akzeptierten Zertifikat signiert ist, das sie freischaltet. Symbian OS prüft beim Installieren des Programms, ob das Zertifikat den Zugriff auf die Capability gestattet. Da sie fest in der Applikation verankert ist, lässt sie sich zur Laufzeit nicht ändern.

Drei Klassen fassen die Capabilities zusammen, was ein mehrstufiges Rechtesystem ermöglicht: User, Extended und Manufacturer Approved. Dadurch erhalten Anwendungen nur Zugriff auf die benötigten APIs.

Das letzte Wort hat der Hersteller

Auf der untersten Stufe finden sich die User Capabilities. Ihrer Verwendung muss der Nutzer zustimmen, damit er die Anwendung installieren kann. Sie enthalten *LocalServices* (unter anderem Bluetooth- und Infrarot-Nutzung), *Location* (Ortsbestimmung), *NetworkServices*, *UserEnvironment* (unter anderem Kamerazugriff), *ReadUserData* (Lesezugriff auf Adressdaten et cetera) und *WriteUserData*.

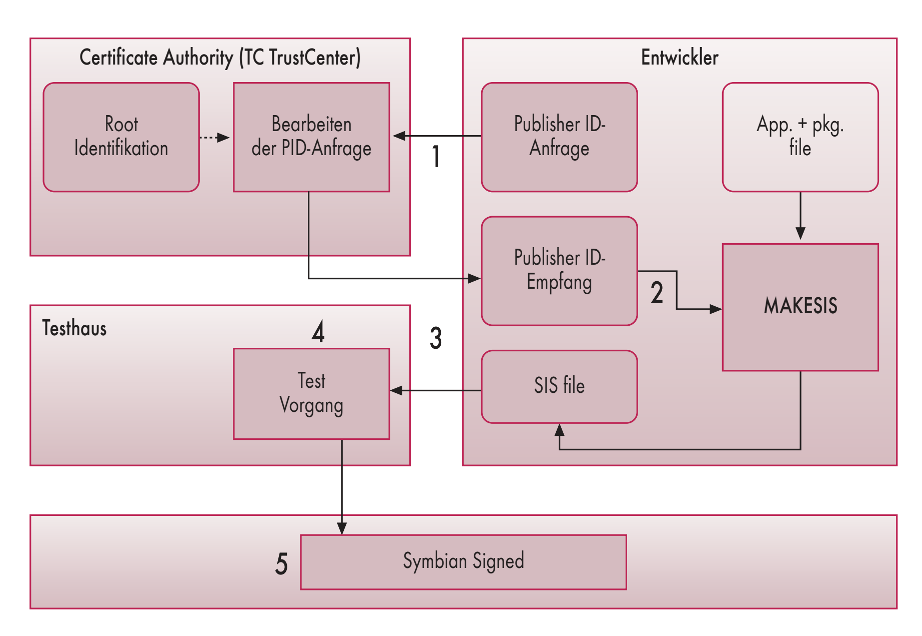
Extended Capabilities enthalten zusätzlich einige als kritisch eingestufte Funktionen. Den Zugriff auf sie kann nur ein Symbian-Signed-Zertifikat erlauben. Zu dieser Klasse gehören *PowerMgmt*, *ReadDeviceData* (Lesen vertraulicher Netzbetreiberdaten et cetera), *TrustedUI* (Eingabe von Passwörtern) und *SwEvent* (Simulation von Eingaben).

In der Klasse der Manufacturer Approved Capabilities befinden sich die mit dem größten Risiko behafteten, da sie nahezu das gesamte System offenlegen. Rechte an ihnen kann nur der Gerätehersteller gewähren. Zu dieser Klasse gehören *CommDD* (direkter Zugriff auf alle Kommunikationstreiber), *DiskAdmin*, *AllFiles* (Lesen des gesamten Dateisystems, Schreiben in private Ordner) und *TCB* (Schreibzugriff auf alle ausführbaren Dateien). Rechte an den beiden letzten werden nach besonders strengen Kriterien (in der Regel eine Analyse des Quellcodes) vergeben, da sie Zugriff auf das komplette System erlauben. Gerätehersteller haben insbesondere in der Klasse der Manufacturer Approved Capabilities einen Auslegungsspielraum.

Zentrales Element der Platform Security ist die Signierung der Anwendung mit einem Zertifikat. Nur so lässt sie sich installieren – sogar, wenn sie keinen Zugriff auf Capabilities benötigt. Ein Entwickler kann seine Anwendung mit einem selbst erstellten Zertifikat signieren, beispielsweise mit den Werkzeugen des Symbian SDK. Ein solches Zertifikat ist kostenlos und der Signaturprozess sehr schnell, da kein Umweg über die Symbian-Signierungsstelle nötig ist. Allerdings erlaubt ein eigenes Zertifikat nur Zugriff auf die User Capabilities, und beim Installieren einer so signierten Anwendung warnt das Gerät vor möglichen Schäden. Gegebenenfalls zeigt es die Capabilities, auf die die Anwendung Zugriff verlangt. Für kommerzielle Anwendungen ist das nicht sinnvoll.

Nur bei Symbian Signed gibt es Zertifikate, die Rechte an sämtlichen Capabilities gewähren. Mit ihnen versehene

Anwendungen lassen sich ohne Warnhinweis auf dem Gerät installieren. Um eine solche Signatur zu erwerben, muss sich der Entwickler beziehungsweise die Firma durch die von einer Certificate Authority (CA) ausgegebene ACS Publisher ID eindeutig identifizieren. Zurzeit akzeptiert Symbian nur TC Trustcenter als CA, wo es die Publisher IDs mit einjähriger Gültigkeit für 200 US-$ gibt.



Fünf Schritte führen den Entwickler zur zertifizierten Symbian-Anwendung (Abb. 1).

Zertifikate mit und ohne Begründung

Voraussetzung für die endgültige Signierung ist der Test der Anwendung durch eine von drei Firmen: Mphasis (Shanghai), NSTL (Blue Bell, USA) und Sogeti (Grenoble). Der Preis dafür hängt von den benötigten Capabilities ab; er liegt zwischen 180 und 500 US-$.

Auch der Signierungsprozess verändert sich je nach den erforderlichen Capabilities. Reicht die User-Klasse, erfolgt die Ausstellung des Zertifikats nach Bestehen einiger einfacher Prüfungen: Lässt sich das Programm fehlerlos installieren und entfernen, speichert es seine Daten an der richtigen Stelle und so weiter. Komplizierter gestaltet sich die Signierung, wenn die Anwendung Zugriff auf Extended Capabilities braucht. Dann muss ein begleitendes „Declarative Statement“ diese Anforderung erklären. Zusätzlich zum Üblichen prüft das Testhaus, ob dieses Begehren gerechtfertigt ist, die Anwendung keinen Schaden anrichtet und wirklich nur die angegebenen Capabilities anspricht. Es erledigt wie vorher den gesamten Prozess.

Braucht ein Programm Zugriff auf Manufacturer Approved Capabilities, kommt der Gerätehersteller ins Spiel. Wiederum muss der Entwickler dem Testhaus eine Liste der angesprochenen APIs samt Begründung liefern. Es nimmt Kontakt mit dem Hersteller auf und wartet auf die Freigabe der Capabilities durch ihn. Neben den Symbian-Signed-Kriterien prüft es die Anwendung nach seinen Anforderungen. Das kostet mehr und dauert länger als in den beiden anderen Fällen. In der Regel muss der Entwickler vorher mit dem Gerätehersteller in Kontakt treten, da er auch zum Entwickeln ein Zertifikat mit passenden Capabilities benötigt, das er nur dort bekommt.

Freeware- und Open-Source-Entwickler können ihre Anwendungen kostenlos von Symbian Signed signieren lassen. Da sie keine ACS Publisher ID benötigen, entstehen gar keine Kosten. Die Installation einer so signierten Anwendung erfolgt allerdings mit dem Hinweis, dass sie Freeware sei. Das soll den Missbrauch des kostenlosen Angebots verhindern. Theoretisch darf Signed Freeware für Symbian jede Capability verwenden. Es dürfte aber nahezu ausgeschlossen sein, dass ein Hersteller Rechte an Manufacturer Approved Capabilities an Freeware-Entwickler vergibt. Diese Signierung ist daher nur sinnvoll, wenn die Anwendung Rechte an Extended Capabilities benötigt. Spricht sie nur User Capabilities an, ist die Selbstsignierung vorzuziehen – die Freeware-Signierung hat bei Symbian zurzeit eine niedrige Priorität und dauert deshalb unvorhersehbar lange.

Entwicklerzertifikate sind grundsätzlich nur für Tests während der Entwicklungsphase erlaubt und an die IMEI (International Mobile Equipment Identity) des Telefons gekoppelt. Aus diesem Grund erscheint vor der Installation einer so signierten Anwendung eine Warnung. Jedoch kann sie der Anwender wie bei selbstsignierten Programmen wegklicken und den Prozess fortsetzen. Für Entwicklerzertifikate wurden die User und Extended Capabilities zusammengefasst. Jedes hat deshalb automatisch Rechte an Capabilities aus diesen beiden Gruppen – nicht jedoch an der Manufacturer-Approved-Klasse.

Im Fünfersprung zu den Rechten

Fünf Schritte sind für die Signatur einer Applikation ohne Manufacturer Approved Capabilities nötig (s. Abb. 1):

– Der Entwickler beantragt eine ACS Publisher ID bei TC Trustcenter, die er für beliebig viele Signierungen über Symbian Signed nutzen kann. Eine Publisher ID ist unter Umständen schon für die Beantragung eines Entwicklerzertifikats notwendig, daher erfolgt dieser Schritt in der Regel vor dem Symbian-Signed-Prozess.

– Das Symbian-Tools *makesis* signiert die Programmdatei mit der Publisher ID.

– Per Symbian-Signed-Portal bekommt das Testhaus diese signierte SIS-Datei übergeben, gegebenenfalls samt einer Erklärung zu den beantragten Capabilities. Nach Prüfung der Publisher ID und der Signatur beginnt das Testen der Anwendung.

– Ist es erfolgreich abgeschlossen, leitet das Testhaus die Anwendung an TC Trustcenter weiter, das sie mit dem endgültigen von allen Symbian-Smartphones erkannten Zertifikat signiert.

iX-TRACT

- Symbian OS und Windows Mobile setzen auf verschiedene Modelle zum Schutz mobiler Geräte vor schädlichen Anwendungen.
- Symbian regelt den Zugriff auf APIs durch ein abgestuftes System von Capabilities und zugeordneten Zertifikaten.
- Windows Mobile verwendet Geräteeinstellungen, die den Anwender sogar an jeder Softwareinstallation hindern können.

– Anschließend geht die Anwendung zurück an das Testhaus. Es unterrichtet den Entwickler über die Signierung der Anwendung, die zum Download auf dem Symbian-Signed-Portal bereitsteht.

Nach Abschluss dieses Vorgangs verliert die signierte Installationsdatei durch jede Änderung ihre Gültigkeit. Daher sollten Anwendungen vor dem Signieren gründlich getestet sein.

Das Sicherheitsmodell schützt nicht nur gefährdete APIs, sondern auch System- und private Daten. Prinzipiell soll eine Anwendung keinen Zugriff auf Systemverzeichnisse oder die Daten anderer Programme erhalten – das Betriebssystem sperrt sie sozusagen in ihrem eigenen Bereich des Dateisystems ein. Dieses Data Caging ist automatisch für alle Programme aktiv und greift in anderem Umfang auch für solche mit umfassenden Capabilites.



Windows Mobile

Microsoft hat bei Windows Mobile darauf geachtet, dass die Entwicklung von Anwendungen der auf dem Desktop so weit wie möglich ähnelt. Wer bereits Windows-Programme in C++ oder mit dem .Net-Framework geschrieben hat, sollte sich leicht auf die Mini-Variante umstellen können. Entwickler müssen allerdings auch das aus mehreren Komponenten bestehende Sicherheitsmodell verstehen: Security Roles (Sicherheitsrollen), Security Policies (Sicherheitsrichtlinien) und Zertifikate samt Signierung.

Windows Mobile erlaubt es, mit Richtlinien und Rollen die Gerätesicherheit direkt einzustellen. Dadurch kann ein Hersteller oder Netzbetreiber beispielsweise festlegen, dass nur Anwendungen mit einem gültigen Zertifikat laufen und sie keine Geräteeinstellungen verändern dürfen. Je nach Einstellung lässt sich Windows Mobile so sehr sicher machen. Andererseits muss der Entwickler deshalb mit unterschiedlichen Sicherheitskonfigurationen rechnen.

Theoretisch vermögen es Hersteller und Netzbetreiber sogar, die Installation jeder weiteren Anwendung zu verhindern. Diese massive Einschränkung würde allerdings die Attraktivität von Windows Mobile deutlich senken. Eine Totalsperre des Geräts dürfte daher nur bei Firmengeräten infrage kommen, vor denen die Administratoren die Netzinfrastruktur schützen möchten.

Bei Windows Mobile spielen die 43 Configuration Service Provider (CSP) eine ähnlich zentrale Rolle wie Capabilites bei Symbian. Sie gruppieren Geräteeinstellungen, Anwendungen sowie APIs und können nahezu alle Betriebssystem- und Gerätefunktionen steuern. Beispielsweise enthält der Bluetooth-CSP alle zum Ansprechen des Bluetooth-Moduls nötigen APIs; der Security Policy CSP versammelt alle Sicherheitsrichtlinien von Gerät und Betriebssystem. Eine solche Richtlinie kann erlauben (allow) oder verbieten (deny). Für Entwickler sind nur vier von ihnen relevant:
– Unsigned Applications Policy zum Ausführen unsignierter Anwendungen (Default: erlaubt);
– Unsigned CABS Policy für das Installieren unsignierter CAB-Dateien (Default: erlaubt);
– Unsigned Prompt Policy zur Nachfrage beim Installieren unsignierten Codes (Default: erlaubt, Dialog erscheint);
– Privileged Applications Policy zum Aktivieren des Zugriffsmodells.

Für das Verständnis dieser Aufzählung ist ein Ausflug zu den Sicherheitsrollen erforderlich.

Eine Security Role ist ein Nutzer mit bestimmten Rechten. Nahezu jeder Funktion des Geräts und des Betriebssystems ist eine solche Rolle zugewiesen – so auch den Security Policies und jedem Configuration Service Provider. Das bedeutet, dass nur ein Nutzer mit den entsprechenden Rechten die Einstellungen der jeweiligen Gerätefunktion ändern kann.

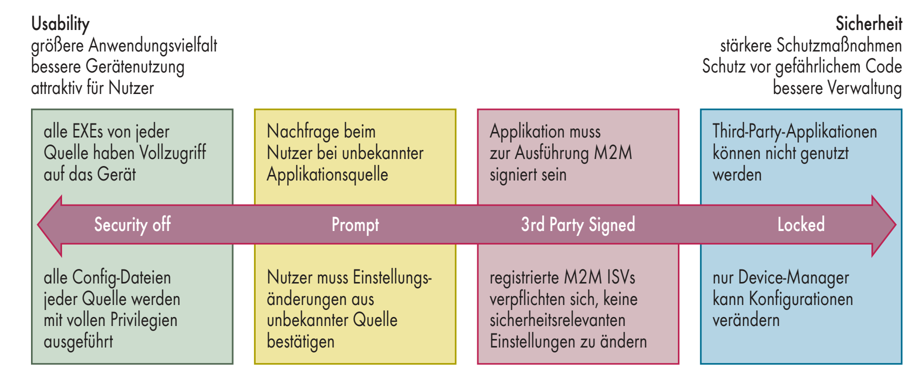
Windows Mobile kennt genau ein Dutzend Security Roles. Die drei wichtigsten sind:
– *SECROLE_MANAGER* mit unbeschränktem Zugriff auf Systemressourcen; kann fast alle Richtlinien ändern und ist meist nicht der Gerätenutzer.
– *SECROLE_USER_AUTH* ist üblicherweise die Rolle des Nutzers. Dieser authentifizierte Anwender hat Zugriff auf die zugeordnete Systemressource.
– *SECROLE_OPERATOR* ist die Rolle des Netzbetreibers mit Zugriff auf die zugeordnete Systemressource.

Nur ein Benutzer mit Manager-Rolle darf Richtlinien ändern. Deshalb müssen sich Entwickler darauf einstellen, dass ihre Kunden die ursprünglichen Sicherheitsrichtlinien nicht anpassen können. Auf den meisten Geräten liegen bei der Auslieferung die oben genannten Standardeinstellungen vor, sodass sich auf ihnen unsignierte Anwendungen ausführen lassen. Allerdings erscheint eine Warnung vor der Installation oder Ausführung, die der Nutzer wegklicken muss.

Sicherheitsmodell je nach Gerät

Windows Mobile kennt außerdem die beiden Permission Models (Zugriffsmodelle) One- und Two-Tier, von denen eines nach der Privileged Applications Policy standardmäßig aktiviert ist. Pocket PCs (mit oder ohne Telefonfunktion) nutzen nur das erste, während Smartphones zwar beide Modelle beherrschen, jedoch ab Werk als Two-Tier-Gerät konfiguriert sind.

Analog zu den Zugriffsmodellen gibt es zwei Verfahren zum Ausführen von Anwendungen unter Windows Mobile: privilegiert und normal. Nur privilegierte Anwendungen verfügen über die *SECROLE_MANAGER*, haben vollen Zugriff auf das Dateisystem sowie die Registry und dürfen jede API verwenden. Alle anderen Anwendungen dürfen sogenannte Trusted APIs nicht benutzen und haben weder Zugriff auf Systemdaten noch auf geschützte Bereiche der Registry. Ob eine Anwendung privilegiert oder normal läuft,



Zwischen vollen Rechten für jedes Programm und der Unmöglichkeit, Anwendungen zu installieren: Windows-Mobile-Geräte lassen sich individuell konfigurieren (Abb. 2).

hängt primär von ihrer Signierung und dem Zugriffsmodell des Geräts ab.

One-Tier-Geräte bieten keine echte Rechteverwaltung: Sie können eine Anwendung nur ausführen oder es lassen. Ist sie mit einem bekannten Zertifikat signiert, installiert das Betriebssystem sie automatisch ohne Nachfrage als privilegierte. Fehlt das Zertifikat oder ist es unbekannt, bestimmt die Security Policy das Verhalten des Geräts: In der Standardeinstellung reicht die Erlaubnis des Benutzers für das Installieren und Ausführen. Das Programm erhält dadurch Privilegien einer signierten Anwendung – also vollen Zugriff auf das Gerät.

Geräte mit dem Two-Tier-Zugriffsmodell vermögen Anwendungen sowohl mit privilegierten als auch mit normalen Rechten auszuführen. Mit einem bekannten Zertifikat einer „Privileged Execution Trust Authority“ signierte behandeln sie wie One-Tier-Geräte, also als privilegierte. Diese kostenpflichtigen Zertifikate werden nur nach Erfüllung bestimmter Kriterien bereitgestellt (mehr dazu später).

Nicht alle Zertifikate sind gleich

Alle anderen Anwendungen laufen nur mit normalen Rechten. Dazu gehören unsignierte und solche mit einem anderen als dem privilegierten. In den ersten beiden Fällen erscheint die erwähnte Warnung, die der Nutzer bestätigen muss. Bei Two-Tier Geräten bekommen nur Anwendungen die Managerrolle, die privilegiert laufen dürfen.

Allerdings verwenden nicht alle Geräte die Standardeinstellung, da jeder Netzbetreiber und Administrator sie ändern kann. Das führt für Entwickler zu Schwierigkeiten, da weder sie noch die Anwender Sicherheitseinstellungen beeinflussen dürfen. Benötigt ein Programm privilegierte Rechte, führt kein Weg an einer kostenpflichtigen Signierung vorbei. Nur sie stellt sicher, dass sowohl One- als auch Two-Tier-Geräte es mit gleichen Rechten ausführen.

Aus den vielfältigen Kombinationsmöglichkeiten der Security Policies ergeben sich vier gebräuchliche Sicherheitseinstellungen (s. Abb. 2).

Die oben beschriebene Standardeinstellung der meisten Windows-Mobile-Geräte ist *Prompt*, also die Nachfrage beim Nutzer, ob er eine unsignierte oder aus unbekannter Quelle signierte Anwendung installieren und ausführen will. Unter dieser Stufe befindet sich nur *Security off*: So konfigurierte Geräte installieren und führen jede Anwendung ohne Nachfrage aus. Sinnvoll ist das nur für Testmodelle.

Eine Stufe über *Prompt* steht *3rd Party Signed*, gelegentlich „Mobile2-Market locked“ genannt. Auf Geräten dieser Sicherheitsstufe lässt sich nur Software nutzen, die mit einem bekannten Zertifikat signiert ist. In der höchsten Stufe *Locked* sind alle Mobile2Market-Zertifikate entfernt, was das Ausführen unerwünschter Drittanwendungen verhindert. Allerdings können sich auf dem Gerät Zertifikate des Herstellers, des Netzbetreibers oder eines Unternehmens befinden. Viele Firmen nutzen diese Einstellung, um die Installation von Fremdsoftware zu verhindern.

Die Signierung einer Anwendung durch eine offizielle Certification Authority garantiert das privilegierte Ausführen der Anwendung auf den meisten Geräten. Ausgangspunkt dafür ist Mobile2Market – Microsofts Gegenstück zu Symbian Signed. Nur ein Zertifikat aus diesem Programm stellt sicher, dass sie auf Two-Tier-Geräten privilegiert läuft.

Reichen dem Programm normale Rechte, erledigt eine CA den Prozess komplett. Braucht es Zugriff auf privilegierte APIs, muss der Hersteller via Mobile2Market Microsofts Genehmigung einholen. Die beiden zulässigen CAs, Verisign und Geotrust, können Anwendungen sowohl für jeden Zugriff signieren. Ähnlich wie bei Symbian Signed braucht man als Erstes eine ACS Publisher ID. Sie dient zum Signieren des Programms mit einem Werkzeug aus dem Windows Mobile SDK. Das Ergebnis erhält die CA, die den Rest erledigt.

Während Symbian-Kunden immer die Signierung der kompletten Anwendung bezahlen, berechnet Mobile2Market einen Betrag für jede einzelne zu signierende Datei – dazu gehören alle EXE-, DLL-, MUI-, CAB- und CPL-Dateien. Jede löst einen „Signing Event“ aus. Ein Preisvergleich lohnt sich durchaus: Das Startpaket mit Publisher ID und 10 Signing Events kostet bei Geotrust 295 und bei Verisign 400 US-$. Weitere Signing Events gibt es in Hunderter-Pakten, mit Mengenrabatt bei steigender Abnahme. Bei diesem Modell können die Kosten für Anwendungen aus vielen Dateien schnell explodieren. Anders als bei Symbian gibt es jedoch keinen Test der Software vor dem Signieren. Das Zertifikat bestätigt also nur den Urheber der Anwendung.

Allerdings bietet Mobile2Market die „Application Logo Certification“, bei der nach bestimmten Richtlinien entwickelte Anwendungen nach der Untersuchung durch ein akzeptiertes Testhaus (zurzeit QualityLogic, NSTL oder Veritest) ein Logo erhalten – Kosten etwa 600 US-$ kostet.



Fazit

Symbian konzentriert sich auf die Signierung und den Schutz kritischer Gerätefunktion: Nur durch die Signierung mit passenden Rechten ausgestattete Programme dürfen auf wichtige APIs zugreifen. Microsoft hingegen legt besonderen Wert auf eine individuelle und maßgeschneiderte Sicherheitseinstellung der Geräte für Geschäftskunden. Dadurch lässt sich sogar die Installation fremder Anwendungen gänzlich unterbinden.

Die meisten Geräte sind jedoch wesentlich laxer konfiguriert, und man kann jede Anwendung auf ihnen installieren. Dies zeigt das grundsätzliche Dilemma eines Entwicklers für Windows Mobile: Da er die Konfiguration der Geräte nicht kennt, kann er nie gewährleisten, dass seine Software auf allen läuft.

Symbian-Entwickler müssen sich damit nicht beschäftigen. Ihr Sorgenkind ist die Plattform Symbian Signed, die in der Vergangenheit durch schlechte Erreichbarkeit und lange Bearbeitungszeiten auffiel. Das hat sich zwar inzwischen gelegt, zeigt aber einen Haken des Konzepts: Ein überlastetes Portal schneidet alle Entwickler vom System ab.

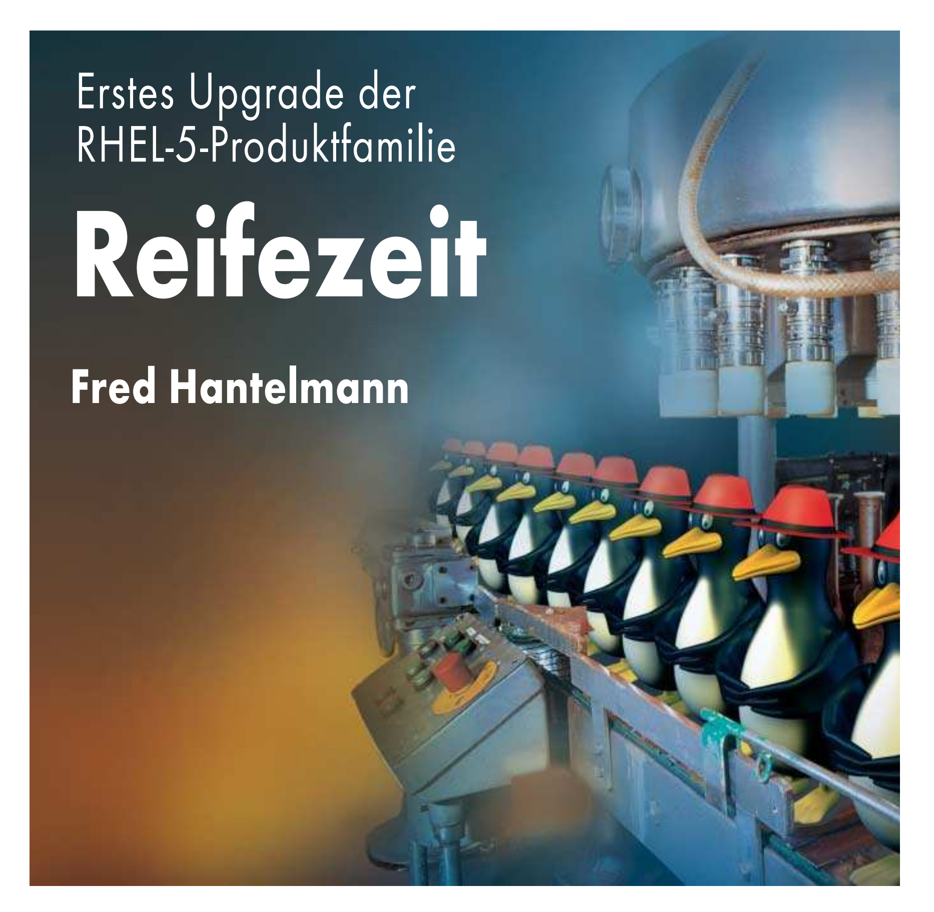
Zudem erschwert Symbian Entwicklern freier Software die Arbeit. Die eigentlich hervorragende Idee, Zertifikate dafür auf demselben Weg wie alle anderen zu verteilen, scheitert an der schlechten Erreichbarkeit und dem trödeligen Verfahren. Wer freie Software für Windows Mobile entwickelt, braucht kein Zertifikat, da sie ohnehin auf der Mehrheit der Geräte laufen wird. (ck)

RAYKO ENZ

ist geschäftsführender Gesellschafter der SIC! Software GmbH und verantwortlich für die technische Leitung des Unternehmens.

JÖRG WEBER

ist bei der SIC! Software GmbH im Bereich Dokumentation und Usability tätig.



Erstes Upgrade der RHEL-5-Produktfamilie

Reifezeit

Fred Hantelmann

Mit dem Einsatz neuer Betriebssystemversionen halten sich erfahrene Admins gern bis zum ersten Servicepack zurück. Für die 5er-Serie seines Enterprise Linux hat Red Hat dieses jetzt vorgestellt. *iX* klärt, ob es reif für den Unternehmenseinsatz ist.

Kommerzielle Linux-Distributionen wollen heuer alle Voraussetzungen für produktiven Einsatz im Unternehmen bereitstellen. Sie bündeln ein breites Spektrum von Open-Source-Programmpaketen und versprechen, dass Kunden damit universelle Arbeitsplatz- und Serversysteme aufsetzen können. Eigenentwicklungen wie Installations- und Administrationstools sollen lokal und am liebsten auch plattformübergreifend die effiziente Konfiguration einzelner Systeme sowie kompletter Systemlandschaften unterstützen.

Darüber hinaus gewähren sie langfristige Produktpflege mit zyklischen Verbesserungen im Bereich der Hardwareunterstützung sowie konsequente Bereinigung aufgefallener Fehler und Sicherheitslöcher. Red Hat beweist dies immerhin seit Mitte 2002 mit seinem RHEL Version 2.1 AS. Kompatibilität mit neuer Hardware verleiht die Softwareschmiede ihren Releases durch Rückwärtsportierung aktueller Kernel-Treiber auf die produktspezifische Kernel-Version – bis die Major-Version aus dem Support-Vertrag herausfällt.

Bedingt durch den ungehemmten Innovationstrieb der Hardwarehersteller ist daher früher oder später der OS-Wechsel unausweichlich. Je früher, desto besser, denn den Bezugspunkt für den Wartungszeitraum legt der Hersteller auf den Termin der Erstausgabe. Dennoch koppeln Unternehmen ihre Wechselbereitschaft oft an die Verfügbarkeit des ersten Servicepacks, und das hat Red Hat nun für RHEL 5 freigegeben. Der Artikel klärt die Produktreife für den Unternehmenseinsatz; Neuerungen gegenüber der Version 5.0 fasst der Kasten „Mehrwert in RHEL 5.1“ zusammen.

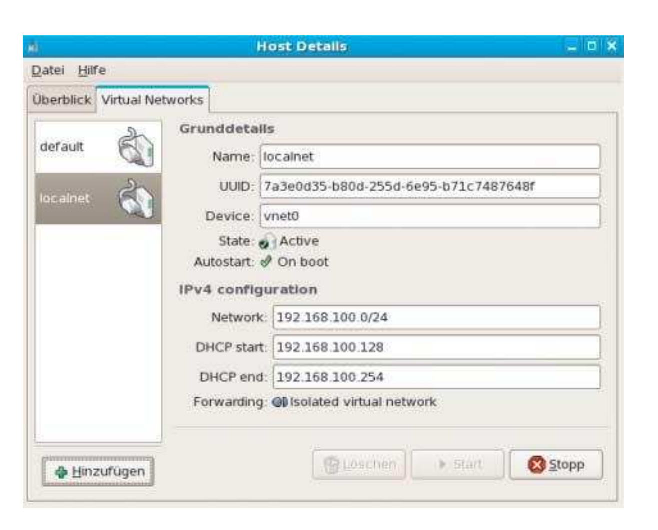
Red Hat fertigt sein Enterprise Linux seit Version 5.0 für zwei Zielgruppen: Die Client-Version, nunmehr als „RHEL Desktop“ im Programm, zielt auf Arbeitsplatzsysteme in 32-Bit- oder 64-Bit-Architektur (x86/x86_64). Server-Distributionen bieten die Amerikaner zusätzlich für Itanium, PowerPC und IBMs System z. Innerhalb der Client- und Server-Produkte legen Funktionsgruppen (Repositories) den Leistungsumfang der jeweiligen Distribution fest. Kunden mit Zugang zum Red Hat Network (RHN) erhalten den Zugriff auf Updates nur innerhalb ihrer abonnierten Repositories.

Bei den Desktop-Lösungen bündeln die Gruppen *Client* und *Workstation* RPM-Pakete zur Bewältigung von Aufgaben aus den Bereichen Office und Multimedia sowie Softwareentwicklung. Im Server stellt stattdessen das *Server*-Repository RPMs für Softwareentwicklung und Webserver bereit. *Virtualization* wiederum ist für beide Zielgruppen verfügbar, jedoch nicht für Power-Prozessoren und auch nicht für IBMs System z. Ein Manko ist das allerdings nicht, denn zu letzteren Systemen hat deren Hersteller eine eigene Virtualisierungslösung im Programm.

Zwei weitere Repositories (*Cluster* und *ClusterStorage*) gibt es nur für die Server-Versionen, und das auch nur zu den Produkten für x86-, x86_64- und Itanium-CPUs. Grob gesagt dienen die Komponenten aus *Cluster* dem Aufbau von hochverfügbaren Systemen in einer Cluster-Architektur oder per Load-Balancer skalierbaren Serverfarm. *ClusterStorage* hingegen liefert die Software zum Verschmelzen mehrerer verteilt vorhandener Massenspeicher zu einem globalen Dateisystem (GFS) mit darüber in Software gelegtem Zugriffsmanagement. GFS Version 2 ist als Technology-Preview verfügbar und will ein kostengünstiges Dateisystem bilden, das speziell auf Cluster-Anforderungen zugeschnitten ist und insbesondere einen zuverlässigen Shared-Storage liefert.

Nur mit Nummer wirklich sinnvoll

Mit der Beschaffung von RHEL 5.1 erhält der Kunde zwar Zugriff auf sämtliche Repositories für die Produktvariante zu seiner Plattform, Updates gibt es aber nur für den abonnierten Part. Selbst die Grundinstallation ist in diesem Bereich restriktiv: Das Installationswerkzeug Anaconda fragt einleitend eine Installationsnummer ab, die den Paketumfang des Abonnements kodiert. Ohne gültige Installationsnummer gelingt nur das Aufspielen der Core-Komponenten, also der Bestandteile des Server- oder des Client-Repositories. Nachträgliche Ergänzungen des ursprünglich installierten Softwareumfangs sind hingegen möglich.



Isolierte virtuelle Netze operieren nur Host-lokal und stehen mit keinem physikalischen Gerät in Verbindung (Abb. 1).

Einem Kopierschutz kommt dieses Verfahren keinesfalls gleich. Der Hersteller begründet diese Vorgehensweise damit, dass der Kunde in jedem Fall ein abgestimmtes Linux vorfinden soll. Wer etwa die Virtualisierung nicht abonniert hat, riskiert laut Red Hat nach einem Online-Update ein inkonsistentes Betriebssystem, da er auf die Updates zu diesem Repository keinen Zugriff hat. Wer ganz auf Updates verzichten und trotzdem den kompletten Softwarevorrat von RHEL 5.1 nutzen möchte, kann ersatzweise die Release-Notes der öffentlich zugänglichen Beta zum Produkt studieren und Anaconda einen der darin abgedruckten Installationsschlüssel nennen.

Anaconda setzt neue Systeme über ein lokales CD-/DVD-Medium, auf lokaler Festplatte befindlichen ISO-Images oder über im Netz per NFS, FTP oder HTTP bereitgestellten Installationsbaum auf. Updates kann Anaconda ebenfalls ausführen. Laut Release-Notes unterstützt RHEL 5.1 jedoch nur ein Upgrade von RHEL 5.0 oder dem aktuellen RHEL 4 Update 6.

Unbeaufsichtigte Installationen gelingen skriptbasiert unter Bezug auf eine Kickstart-Datei. Zu jeder Neuinstallation erzeugt Anaconda automatisch die Datei */root/anaconda-ks.cfg*, mit der der Administrator das betreffende System unbeaufsichtigt in den Urzustand versetzen kann – fast. Tatsächlich durchläuft jedes System mit aufgespieltem X11 beim ersten Start eine *firstboot*-Sequenz, in der der Administrator nachträglich Datum und Uhrzeit einstellt, Benutzer anlegt, die Firewall konfiguriert et cetera. Diese Änderungen reflektiert die Kickstart-Datei nicht.

Die Display-Konfiguration ist übrigens in RHEL 5.x nicht mehr Bestandteil der Anaconda-Installationsmenüs. Im Test startete das System X11 per *firstboot* mit 1920 × 1440 Bildpunkten auf einem 19-Zoll-Monitor. Um die Kommandos *locate* und *apropos* unmittelbar auf einem neu installierten System nutzen zu können, ist der Aufruf von *updatedb* und *makewhatis* erforderlich.

Wer statt manueller Anpassung einer vorhandenen Kickstart-Datei für das unbeaufsichtigte Installieren weiterer Systeme ein grafisches Werkzeug wünscht, dem bietet RHEL 5.1 das Python-Programm *system-config-kickstart*. Es ist ein optionales Verwaltungstool der Gruppe „Basissystem“ und daher nachträglich zu installieren. Falls vorhanden, findet es der Administrator auf dem Desktop unter „Anwendungen“ im Bereich „Systemwerkzeuge“.

Uneinheitliche Werkzeuge zur Systemverwaltung

Nachträgliches Installieren von Softwarepaketen erfolgt seit RHEL 5.0 via Yellowdog Update Manager (*yum*). Dieser greift je nach Konfiguration auf lokale und entfernte Repositories zu, löst selbsttätig die Abhängigkeiten auf und entpackt mit einem Programmaufruf alle benötigten RPM-Dateien auf das lokale System. Frisch aufgesetzte RHEL-5.1-Systeme kennen zunächst nur den Suchpfad für Debug-Info-Pakete auf Red Hats Servern.

Leider verhinderte im Test die Beschaffenheit des DVD-Verzeichnisbaums den Aufbau einer elementaren *yum*-Konfiguration für dieses Medium. Der Hersteller hat seinen Repository-Deklarationen den Zusatz „xml:base“ mit einem URL-Argument „media://“ gegeben. Die mitgelieferte *yum*-Version 3.0.1 unterstützt diesen Schlüssel noch nicht. Abhilfe schaffte das Binden der DVD und anschließender Aufruf von *createrepo* . am Mountpunkt, gefolgt von *yum clean all* und *yum makecache*.

Dem grafische Paketmanager *pirut* genügt das jedoch nicht. Er gibt sich erst nach Kopieren der DVD auf Festplatte und Neuerstellen aller *repodata*-Verzeichnisse zu den enthaltenen Repositories zufrieden. Die *yum*-Konfiguration muss dann jedes Repository einzeln aufnehmen. Der Kickstart-Editor *system-config-kickstart* schließlich setzt zusätzlich voraus, dass mindestens einer der

Mehrwert in RHEL 5.1

Bezogen auf die Vorgängerversion 5.0 stellt Red Hat mit Freigabe von RHEL 5.1 massive Verbesserungen an der Virtualisierungsschicht in den Vordergrund. Statt Xen 3.0.3 bildet Xen 3.1 die Basis für dieses Aufgabenfeld. Damit einher gehen SMP-Support, Unterstützung der Save-/Restore-Funktionen und Live-Migrationen für vollvirtualisierte Gäste. Das in Python geschriebene Management-GUI *virt-manager* verwaltet nun auch schlafende Gäste und kann virtuelle Netze nebst darauf operierendem DHCP-Server konfigurieren.

Laptops und Desktops sollen von verbesserter ACPI-Unterstützung profitieren, sodass Suspend-to-RAM und Hibernate nun auf neuer und etwas betagterer Hardware gelingen. Das Ext3-Dateisystem darf sich über bis zu 16 TByte erstrecken. Die NFSv4 Funktionen „Replikation“ und „Migration“ sind laut Hersteller in RHEL 5.1 implementiert. Werkzeuge zum Aufbau von iSCSI-Targets liefert Red Hat als sogenannten Technology-Preview über das *ClusterStorage*-Repository.

Weitere Neuerungen in RHEL 5.1 betreffen laut Red Hat Verbesserungen an der Kommunikation mit Windows-Systemen. Das sollen Versions-Updates von Samba auf 3.0.25b, NSS-LDAP auf 253-5 und PAM KRB5 auf 2.2.14 leisten. Im Hinblick auf moderne Sicherheitsanforderungen zählt der Enterprise Security Client *esc* zum Lieferumfang. Andere Neulinge sind: *dnsmasq* (lightweight DNS forwarder plus DHCP Server), *libwpd* (Bibliothek zum Umgang mit Word-Perfect-Dokumenten), *meanwhile* (Lotus Sametime Clone), *nfs4-acl-tools* (NFSv4 Client Tools), *opal* (Open Phone Abstraction Library), *poppler* (PDF-Rendering-Bibliothek), *scsi-target-utils* (Software iSCSI Targets Daemon und Tools) und *svrcore* (Netscapes *svrcore*-Bibliothek).

Schließlich dürfen Open-Source-Puristen nun mit den integrierten Liberation Fonts einen Satz TrueType-OpenType formatierter GPL+-konformer Schriften benutzen, die die geschützten Schriften Times New Roman, Arial und Courier New ersetzen wollen.

Einträge dort mit *[base]*, *[core]* oder *[development]* überschrieben ist.

Ein Administrationszentrum existiert in RHEL 5.1 weiterhin nicht. Stattdessen enthält es zahlreiche *system-config-**-Werkzeuge, die zwar mehrheitlich, aber nicht konsequent unterhalb von „Administration“ im System-Menu zugänglich sind. Abgesehen davon, dass RHEL seit Version 5 keinen Netzwerkboot-Konfigurator mehr enthält, bilden DNS- und Kdump-GUIs die Neuzugänge der Basisausstattung dieser Produktlinie. NIS und LDAP sind in RHEL 5.1 nicht grafisch konfigurierbar. *system-config-bind* als Frontend für die Named-Konfigurationsdateien erwartet einen Internetzugang, um die Root-Level-DNS-Server zu laden. Mit etwas Nacharbeit gelang das auch ohne Internetanschluss: Einspielen des Caching-Nameservers und Erstellen von *named.conf* sowie *named.root.hints* aus den einschlägigen Beispielen konnten das Tool im Test überreden, in einer Laborumgebung den Aufbau eines DNS-Servers zu unterstützen.

Zeitgemäß oder zumindest wünschenswert ist eine kontextsensitiv arbeitende Hilfefunktion zu den Administrationstools. In diesem Punkt hat RHEL 5.1 bisher nur in Ausnahmefällen die passende Antwort: Beispielsweise kennen Drucker- und LVM-GUI nur ein Info-Fenster. Einige Werkzeuge starten den Gnome-Systemdokumentations-Reader *yelp*, andere bemühen den Webbrowser Firefox. Hilfe zum DNS-Tool ist nur als PDF vorhanden.

Virtualisierungsfunktionen aufpoliert

Abweichend von den Release-Notes der RHEL-4.x-Reihe gibt es in den gleichnamigen Dokumenten aus RHEL 5.1 keine Liste der mit dem Update einhergehenden Paketänderungen. Im konkreten Fall sind mehr als 150 Pakete betroffen, darunter auch eine Handvoll neue (siehe „Mehrwert in RHEL 5.1“).

Abschließend noch ein paar Kommentare zu den Neuerungen der Xen-Integration in RHEL 5.1: Das in Python geschriebene grafische Konfigurationstool *virt-manger* nutzt die API von *libvirt* Version 0.2.3 zur Kommunikation mit dem Xen Hypervisor. Damit gelingt das Anzeigen konfigurierter Gast-Domains des angefragten Host, Erstellen neuer paravirtualisierter oder vollvirtualisierter Gäste, Modifikation der Ressourcenzuordnung zu Gästen und Starten, Anhalten sowie Beenden virtueller Instanzen. Snapshots und (Live-)Migrationen unterstützt *virt-manager* nicht. In seiner Lösung benutzt der Hersteller *libvirt*, da diese API neben Xen auch Qemu als Ressourcenscheduler bedienen kann. Qemu selbst ist jedoch nicht Bestandteil der Distribution. Der Versuch, einen PowerPC-Gast für diesen Emulator zu erzeugen, brach im Test mit der Meldung ab, dass */usr/bin/qemu* fehlt. Nachträgliches Erstellen von Qemu 0.9 aus den Sourcen – das gelingt in RHEL 5.1 nur mit *gcc34* – ermöglichte auf einem x86_64-Host immerhin das Booten des PPC-Linux Yellowdog 4.0.1. Eine Installation des OS als Gast gelang im Test nicht.

Grundkonfigurationen neuer Gäste unterstützt *virt-manager* mit einem Wizard-ähnlichen Dialog, in dem der Administrator die initiale CPU- und Speicher-Ausstattung sowie je eine CD-ROM, Festplatte und Netzwerkschnittstelle spezifizieren kann. Initial booten neue Gäste stets vom CD-Medium, das ihnen nach erneutem Boot hingegen nicht mehr zur Verfügung steht. Wer etwa Windows 2000, 2003 oder XP vollvirtualisiert installieren möchte, stolpert über diese Eigenschaft, da das CD-Laufwerk in der zweiten Installationsphase fehlt. Notwendige Umwege, in Form der manuellen Modifikation der zugehörigen Xen-Konfigurationsdatei, finden sich in den Release-Notes zu RHEL 5.1.

Prinzipiell sollte auch ein Bearbeiten der Hardwareausstattung zu einem Gast per *virt-manager* zum gewünschten Ergebnis führen, doch das ist nicht der Fall: Zwar kann der Administrator zusätzliche Festplatten konfigurieren, er hat jedoch keinen Einfluss auf die Qemu-Attribute, die der Gast erhalten soll – in diesem Fall kann er den benötigten Zusatz „:cdrom“ hinter der Laufwerkskennung nicht angeben. Boot-Device und übrigens auch Tastatur-Layout kann *virt-manager* ebenfalls nicht setzen.

Eine willkommene Verbesserung in RHEL 5.1 ist schließlich die optionale Konfiguration isolierter virtueller Netze. Diese operieren nur Host-lokal und stehen mit keinem physikalischen Gerät in Verbindung – gegebenenfalls mit einem lokalen DHCP-Dienst zur Unterstützung. Abbildung 1 zeigt ein Beispiel. Systemintern erscheint das so erstellte Netz einfach als zusätzliche Bridge, bestehend aus einem Tap-Device und daran gebundene VIFs (Virtual Network Interfaces) der teilnehmenden Gäste. Eine Konfiguration von Bridges, die an Vlan-Devices koppeln, unterstützt das Tool hingegen nicht.

Fazit

Wer die Unternehmensreife einer Linux-Distribution über das Dienstleistungsangebot seines Herstellers definiert, also Langzeitpflege, Hotline, Update-Server und auch Hardware, Software und personelle Qualitätsgarantie vermöge von Zertifizierungsschemata in das Zentrum seines Begehrens stellt, der findet in RHEL 5.1 den gewünschten Rahmen. Auch in Sachen Sicherheit und Stabilität der Komponenten kann das Produkt erwartungsgemäß punkten. Letztlich hat Red Hat über genau diese Merkmale im Laufe der Jahre hohes Ansehen erlangt.

Kleinere Unpässlichkeiten, zugegebenermaßen mit spitzem Bohrer aufgedeckt und überwiegend kosmetischer Natur, sollten den Hersteller veranlassen, seine administrativen Werkzeuge zügig zu homogenisieren. Sein beanspruchter Mehrwert gegenüber dem Vorgänger im Bereich Virtualisierung wirkt im Gegensatz zur Einschätzung des Herstellers kaum bahnbrechend, gemessen an dem Potenzial, das Xen und Qemu faktisch liefern. Dass der Endkunde nur mühsam das Distributionsmedium für lokale Paketinstallation nutzen kann, lässt Nachlässigkeiten in der Qualitätssicherung vermuten. (avr)

DR. FRED HANTELMANN

ist als IT-Architekt bei der Online Systemhaus ES+C GmbH tätig.

iX-Wertung

⊕ stabile Kernkomponenten

⊕ ausgereiftes Support-Angebot

⊖ Administrationstools inkonsistent

⊖ keine lokalen Updates vom Installationsmedium

Daten und Preise

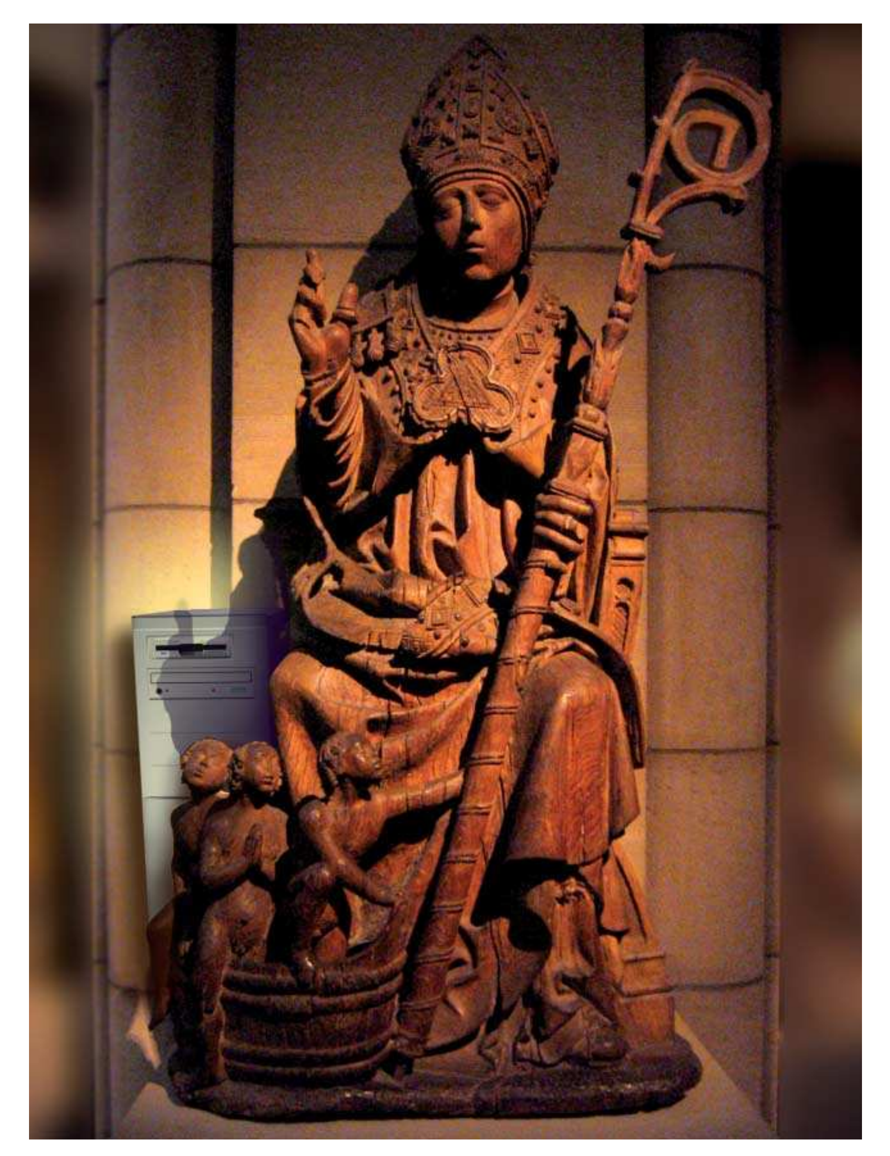
Red Hat Enterprise Linux 5.1

Hersteller: Red Hat, www.redhat.de

Plattformen: x86, x86_64, ia64, PowerPC, System z (Server); x86, x86_64 (Desktop/Workstation)

Preise: Subskriptionsmodell, Desktop ab 60 €, Workstation ab 143 €, Server ab 279 €, Preise pro Jahr für Basic-Variante

Nagios in Version 3.0 freigegeben



Neues vom Schutzheiligen

Sven Velt

Schon in früheren Versionen war das Open-Source-Monitoring-System Nagios ein wichtiger Bestandteil des Admin-Werkzeugkastens. Es ist deshalb Zeit, einen Blick auf die Konzepte und Neuerungen zu werfen.

Das Systemüberwachungswerkzeug Nagios (Network + Agios, griechisch: Heiliger) steht kurz vor der Freigabe der dritten Generation, bei der sich wieder viel „unter der Haube“ verbessert hat. Schon von Anfang an legten die Entwickler Wert auf Modularität und Erweiterbarkeit. Dementsprechend konzentriert sich Nagios im Gegensatz zu anderen Monitoring-Lösungen auf wenige, eingebaute Funktionen – den „Rest“ erledigen Plug-ins beziehungsweise Kommandos, die sowieso auf jedem Unix-System installiert sind.

Zum Aufsetzen eines Nagios-Servers benötigt man das Nagios-Package (siehe „Onlinequellen“ [a]), das neben dem Daemon die CGI-Skripte für das Web-Frontend enthält. Dazu gesellen sich die Check-Plug-ins aus dem „Nagios-PlugIns“-Projekt [b]. Die Entwicklung wurde schon vor Jahren getrennt, da die sauber definierten und einfachen Schnittstellen es meistens ermöglichen, neue Plug-ins mit älteren Nagios-Versionen und umgekehrt zu betreiben. Dies führt letztendlich dazu, dass die Plug-ins wesentlich schneller weiterentwickelt, ergänzt und korrigiert werden können. Selbst andere Monitoring-Lösungen bieten inzwischen Schnittstellen zu den Nagios-Plug-ins an, um von der großen Vielfalt zu profitieren.

Bei der Konfiguration des Nagios-Systems greifen Administratoren größerer Installationen oft entweder auf den guten, alten Texteditor oder auf selbst geschriebene Skripte zurück. Es existieren zwar einige grafische Tools für die Konfiguration, jedoch hat es bisher noch keines geschafft, sich für die verschiedenen Anwendungsszenarien zu eignen. Dies ist direkt auf die vielen Möglichkeiten zurückzuführen, die Nagios bietet.

Konzepte der Konfiguration

Für Nagios ist das grundlegende Objekt der Host. Er hat genau eine IP-Adresse und kann somit praktisch jedes Gerät im Netz darstellen. Via „Host-Check“ lässt sich testen, ob er noch erreichbar ist. Hier verwendet man typischerweise einen Ping – in der Hoffnung, dass übereifrige Firewall-Administratoren ICMP oder Teile davon nicht verboten haben.

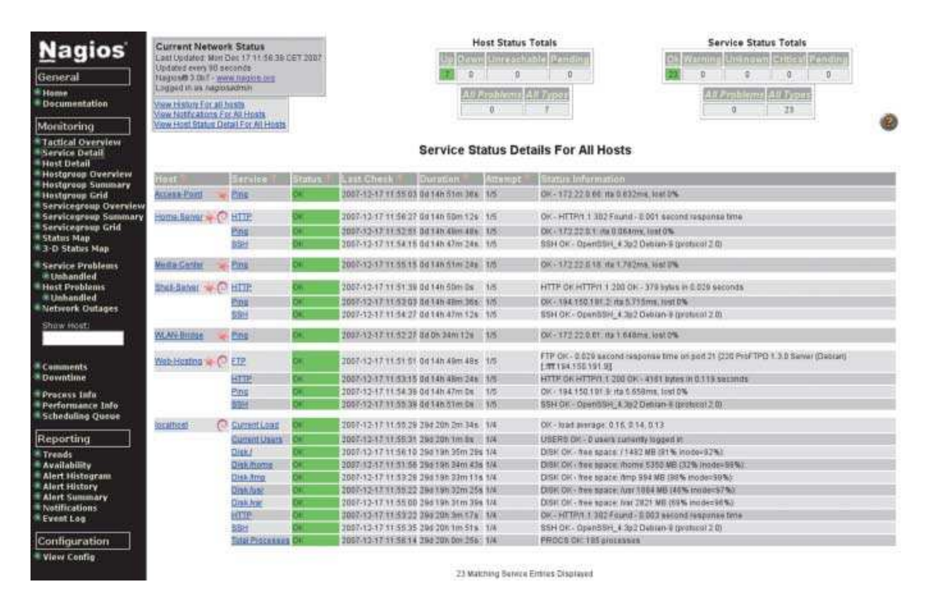
Auf einem Host lassen sich ein oder mehrere sogenannte Services definieren: Beispielsweise ein Test, ob auf einem bestimmten Port ein bestimmter Server lauscht beziehungsweise dessen Protokoll gesprochen wird (HTTP, FTP,

SMTP, IMAP et cetera), eine Überprüfung, wie viel freien Platz eine Partition oder Netzwerk-Freigabe bietet oder ob neue (Sicherheits-)Updates für die Distribution vorliegen. Dabei kann der Admin für jeden Service die Testhäufigkeit festlegen. Als Quasi-Standard hat sich hier ein 5-Minuten-Intervall bewährt. Zum Reduzieren unnötiger Benachrichtigungen kann man bestimmen, wie lange ein Check ein negatives Ergebnis liefern muss, bis Nagios von einem Fehler ausgeht.

Jeden dieser Service-Checks muss der Administrator in Nagios als „Command“ definieren. Dazu registriert er die Nagios-Plug-ins unter beliebigen Namen – teilweise mehrfach mit unterschiedlichen Kommandozeilenparametern. Beispielsweise kann *check_http* aus den Nagios-Plug-ins nicht nur testen, ob ein Webserver antwortet, sondern selbst die Größe, das Alter, den Inhalt der übertragenen Daten oder den HTTP-Statuscode überprüfen. Auch SSL-Webserver kommen nicht zu kurz, und so kann Nagios den Zuständigen informieren, wenn das Zertifikat bald abläuft – ein in der Praxis von vielen Nagios- und Webserver-Administratoren geschätztes Feature.

Jeder Host und jeder Service lässt sich einer Gruppe von Verantwortlichen zuweisen. Diese Zuordnung sorgt einerseits dafür, dass Nagios im kritischen Fall die richtigen Personen informiert und andererseits, dass nicht jeder im Web-Frontend alles sieht, sondern nur Hosts und Services, für die er zuständig ist. Ebenso kann man je „Contact“ festlegen, wann Nagios über Probleme informieren soll. Häufig legt man pro Person mehr als einen „Contact“ an, die zeitlich unterschiedliche Benachrichtigungswege nutzen – tagsüber via E-Mail, nachts und am Wochenende per SMS.

Für die Benachrichtigung bringt Nagios – wie bei den Service-Checks – ebenfalls nichts mit. In der mitgelieferten Konfiguration verlässt sich Nagios auf den im Unix-Umfeld bei jedem Server üblichen Mailserver und verschickt lediglich E-Mails per *mail*-Kommando. Dieses findet wie die Service-Checks als „Command“-Definition seinen Weg in die Konfiguration. Da SMS-to-Mail-Gateways zumindest im Monitoring-Umfeld nicht der Weisheit letzter Schluss sind (wie soll man den Gateway-Rechner erreichen, wenn entweder ein Mailserver oder die Standleitung ausgefallen sind?), ist hier auf jeden Fall Handlungsbedarf angesagt. Den wohl günstigsten Weg zu einer Internet-unabhängigen SMS-Benachrichtigung schafft



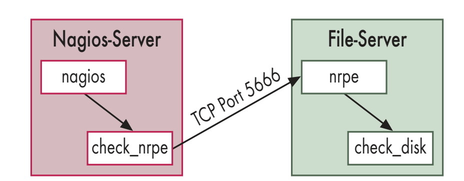
Nagios-Administratoren lassen auch zu Hause das Beobachten nicht sein, hier: „Service-Übersicht“ (Abb. 1).

ein Handy direkt an der seriellen Schnittstelle, das Nagios über Tools wie *Gnokii* [c] oder *scmxx* [d] anspricht. Ähnlich einfach ist die Installation eines Modems oder einer ISDN-Karte, mit denen man sich direkt beim Handy-Provider einwählt und so die SMS abschickt. Als schönste Lösung darf wohl ein GSM-Modem mit Ethernet-Anschluss gelten. Alternative Benachrichtigungsformen, wie Instant-Messaging via Jabber oder Anrufe auf dem Handy lassen sich natürlich ebenfalls realisieren. Wie so oft bei Nagios sind hier nur die Fantasie oder die Zeit des Administrators die begrenzenden Faktoren.

Möchte man sicherstellen, dass jemand bei Störungen tatsächlich handelt, so lässt sich dies über Eskalationsketten realisieren. Sollte der zuständige Administrator oder Techniker nicht innerhalb einer definierten Zeit reagieren, schickt Nagios die nächste oder nächsten Benachrichtigungen an mehr oder andere Personengruppen. Schließlich lassen sich logische Abhängigkeiten konfigurieren. Die häufige Motivation dafür: Das Vermeiden unnötiger Benachrichtigungen, damit wichtige Ereignisse nicht in einem Wust von Meldungen untergehen. So ist

iX-TRACT

- Nagios gehört zum Standardwerkzeugsatz vieler Systemadministratoren.
- Dank seines modularen Aufbaus lässt sich das Open-Source-Monitoring-Tool individuell anpassen und erweitern.
- Eine Parallelisierung der Systemtests verhindert größere Überwachungslücken durch Wartezeiten.



NRPE kümmert sich um die Ausführung eines Plug-ins auf einem anderen Rechner (Abb. 2).

es beispielsweise unnötig, den Zuständigen zu warnen, dass der HTTPS-Zertifikats-Check negativ ausfällt, wenn schon der Webserver nicht erreichbar ist. Teilt man Nagios mit, welche Rechner als Router fungieren beziehungsweise welche Hosts über welche anderen Hosts erreichbar sind, reicht es, wenn Nagios nur den Ausfall eines Routers meldet statt vielleicht 200 ausgefallene Rechner. Dies verschafft im Falle des Falles mehr Übersicht, wo tatsächlich Hand anzulegen ist.

Überwachung anderer Rechner

Neben über das Netz ausgeführten Tests gibt es Daten, die man nur „direkt“ auf dem Rechner abrufen kann, beispielsweise den Füllstand der Partitionen. Viele Monitoring-Lösungen gehen hier den Weg über SNMP. Mit dem Plug-in *check_snmp* kann Nagios dies zwar auch nutzen, bietet jedoch einen wesentlich schöneren Weg: NRPE.

Der „Nagios Remote Plug-in Executor“ oder kurz „NRPE“ [e] besteht aus zwei Teilen: einem kleinen, als Check-Command ausgeführtem Plug-in (*check_nrpe*) für den Nagios-Server sowie einem Daemon. Das Plug-in teilt dem *nrpe*-Daemon auf dem zu überwa-

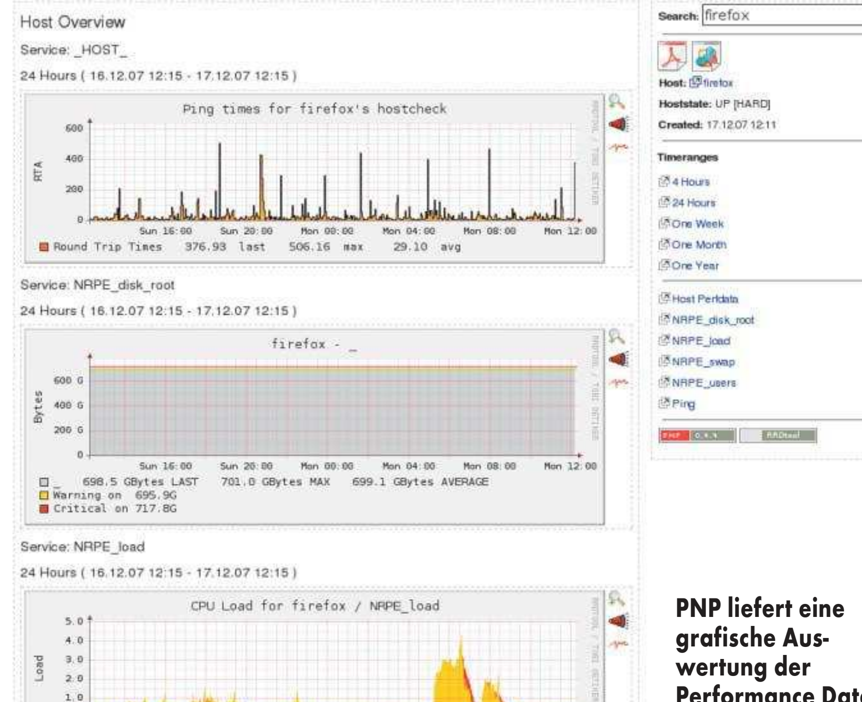
chenden Rechner über eine TCP-Verbindung mit, welches der in *nrpe.cfg* definierten Kommandos gewünscht ist. Kommt die Anfrage von einer zulässigen IP-Adresse, führt der Daemon den hinterlegten Plug-in-Aufruf aus. Das Ergebnis sendet er an das *check_nrpe*-Plug-in zurück. Dieses Vorgehen bedeutet zwar, dass man zumindest eine Plug-in-Auswahl auf jedem zu überwachenden Rechner installieren muss – auf der anderen Seite ist man aber flexibel und kann ohne große Schwierigkeiten weitere (eigene) Plug-ins nachrüsten.

Web-Frontend und External Commands

Läuft der Nagios-Daemon, schreibt er in regelmäßigen Abständen eine Statusdatei ins Dateisystem. Darauf greifen die – im Moment noch in C geschriebenen – CGI-Skripte zu und stellen den aktuellen Stand der zu überwachenden Hosts dar. Über das Web-Frontend lässt sich auch der Nagios-Daemon steuern: So kann man beispielsweise Störungsmeldungen quittieren, Benachrichtigungen und Checks an-/ausschalten oder Kommentare hinterlegen. Über das in der Konfiguration benannte „External Command File“ erreichen die Aktionen den Daemon – genauer: eine regelmäßig ausgelesene Named Pipe. Dieser Weg steht natürlich auch engagierten Administratoren offen, um Nagios mit eigenen Skripten zu steuern (beispielsweise: Wartungsfenster Freitags von 16 bis 18 Uhr via *cron* und Shell-Skript ansetzen).

Zum Web-Frontend bleibt noch zu sagen, dass die Entwickler es ursprünglich mit Nagios 3 durch ein neues, wahrscheinlich in PHP geschriebenes, ersetzen wollten. Da sich dies aber bestimmt noch länger hingezogen hätte und viele auf die neuen Features der Version 3 warten, hat sich Nagios-Vater Ethan Galstadt entschlossen, die Version 3 noch mit einem alten, aktualisierten Frontend freizugeben. Die Basis des neuen Frontends werden die NDOUtils bilden [f], die sämtliche Informationen des Nagios-Daemons in einer Datenbank speichern. Wer schon jetzt mit den NDOUtils testen will, kann dies tun – sie stehen auf der Nagios-Webseite [a] für Nagios 2 und 3 zum Download bereit.

Viele Nagios-Plug-ins (nicht nur aus dem offiziellem Projekt) liefern sogenannte „Performance Data“ oder kurz „Perfdata“ zurück. Es bietet sich zum Erkennen langfristiger Trends ja förmlich an, Ping-Zeiten, Partitionsfüllstände, CPU-Load und Ähnliches grafisch aufzubereiten. Dabei sei allerdings erwähnt, dass Tools wie MRTG, Cacti oder Ähnlichen durch Nagios hier keine echte Konkurrenz erwächst – Monitoring ist eben nicht gleich Graphing. Die meisten Tools setzen zum Archivieren und Darstellen der Graphen auf RRDTool (PNP [g], NagiosGrapher [h]). Einige verwenden es bewusst nicht, um für längere Zeit exakte Werte zu speichern (PerfParse [i]), was allerdings meist auch mit deutlich größeren zu verarbeitenden Datenmengen einhergeht.

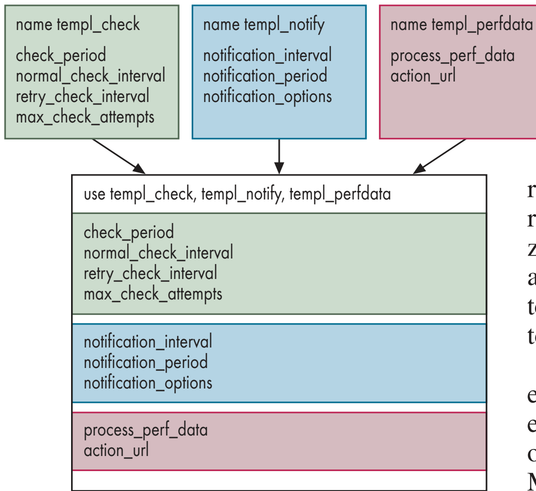


PNP liefert eine grafische Auswertung der Performance Data von Ping, Dateisystemfüllstand und Load (Abb. 3).

Nagios 3 – die Neuerungen

Eine der zentralen und von den meisten Anwendern heiß erwartete Neuerung betrifft die Host-Checks. Bis einschließlich Version 2 prüft Nagios Hosts normalerweise nur, wenn ein Service ausgefallen ist. Die Logik dahinter: Liefert ein Service auf dem Host als Ergebnis ein „OK“ zurück, so muss das System ja funktionieren. Umgekehrt führt Nagios einen Host-Check aus, wenn das Ergebnis nicht OK ist, um festzustellen, ob es sich um einen Service- oder Host-Ausfall handelt. Zwar kann Nagios 2 Host-Checks auch regelmäßig anstoßen, jedoch führen die immer dazu, dass Nagios alle anderen Überprüfungen aussetzt, bis der Zustand des Host geklärt ist. Es prüft dabei im Fehlerfall aber nicht nur den aktuellen Host, sondern alle Hosts in der Netzhierarchie bis zum Nagios-Server selbst – sollten sich hinter dem betroffenen System noch weitere befinden, diese ebenfalls. Dies kann in großen, verzweigten Netzen schnell dazu führen, dass Nagios minutenlang keine Service-Checks mehr ausführt. Um dieses Verhalten in den Griff zu bekommen, behandelt Nagios 3 Host-Checks wie Service-Checks. Es kann sie (aber nicht zwingend) regelmäßig initiieren. Dann sieht Nagios den Status des Hosts für einige Sekunden als gültig an, sodass es keinen weiteren Check ausführen muss. Stellt es jedoch ein Host-Problem fest, überprüft Nagios weiterhin andere betroffene Rechner eventuell ebenfalls, aber eben parallel zu allen sonstigen Aufgaben, ohne anderes zu blockieren. Dieses neue Verhalten bringt, wie schon angesprochen, in großen Umgebungen Verbesserungen, vor allem, wenn dort regelmäßig Hosts nicht erreichbar sind.

Eine weitere, ebenfalls lange ersehnte Verbesserung betrifft die „Timeperiods“. Konnte man bisher nur für Wochentage bestimmte Zeiten definieren, hat Ethan Galstadt dies in Version 3 massiv erweitert. Zusätzlich lassen sich jetzt bestimmte Daten, ein bestimmter Tag im Jahr und gewisse Tage respektive Wochentage im Monat ansprechen. „Erster Montag im Monat“, „vorletzter Samstag“ oder „1. Januar jedes Jahr“



Ein Objekt kann seine Einstellungen durchaus von mehreren Templates erben (Abb. 4).

bereiten jetzt keine Schwierigkeiten mehr. Ebenso lassen sich mit einer einmaligen Aktion pro Jahr Feiertage einpflegen und zugehörigen, Benachrichtigungszeitspannen daran anpassen. Sollte man von einer zweiwöchentlichen Rufbereitschaft überzeugt sein, so lässt sich auch das realisieren.

Bei den Benachrichtigungen kann der Administrator jetzt die Kontakte über Downtime-Ereignisse informieren, wann diese beginnen und enden. Die erste Meldung eines Problems lässt sich um eine definierte Zeitspanne hinauszögern – gerade bei der alten Host-Check-Logik wäre es manchmal ein Segen gewesen, schlecht angebundenen Hosts ein paar Minuten zu geben, sich eventuell wieder zu fangen.

Musste der Administrator bisher sowohl für den Host als auch den Service die Benachrichtigungsoptionen setzen, so erben Services diese bei nicht vorhandener individueller Definition nun vom jeweiligen Host. Sollte es also einen Rechnerpark geben, für den vom Betriebssystem bis zur darauf laufenden Applikation ein Team zuständig ist, spart das wieder Konfigurationsarbeit. Genauso lassen sich Services auf mehreren Hosts definieren, deren Benachrichtigungseinstellungen Nagios über die Hosts verschieden auflöst.

Für das Web-Frontend kann man nun auch Kontaktpersonen anlegen, die sich zwar den aktuellen Zustand ihrer Host und Services ansehen können, aber keine Kommandos absetzen dürfen. Dies ist von Bedeutung, hat man Kundensysteme in sein Nagios aufgenommen und gibt den Kunden einerseits die Möglichkeit, sich den aktuellen Zustand anzusehen, möchte aber andererseits verhindern, dass sie aus purem Unwissen mit falschen Einstellungen das Monitoring negativ beeinflussen. Andersherum geht es auch: Nur das Web-Frontend freischalten (inklusive Steuerungsmöglichkeit), aber keine Benachrichtigungen absetzen. Dies ließ sich zwar schon in Nagios 2 realisieren, aber nicht über Konfigurationsparameter, sondern nur über geschickt gewählte Benachrichtigungs-Commands.

Auch in Sachen Gruppenbildung gibt es Neues: War es bisher nur möglich, einen Host in Hostgroups zu stecken oder den Hostgroups zu sagen, welche Mitglieder (*members*) sie haben, so lassen sich jetzt auch Gruppen in Gruppen zusammenfassen. Dazu führt Nagios 3 bei den Hostgroups die Option *hostgroup_members* ein. Äquivalentes gilt für Service- und Contactgroups.

In Host- und Kontakt-Gruppen bietet der neue Operator „!“ die Option, Ausnahmen zu definieren. Man kann damit erstmals einzelne Hosts oder Kontakte aus einer größeren Auswahl wieder herausnehmen. Genauso führt Nagios 3 für Template-vererbte Einstellung die Operatoren „+“ und „null“ ein, um beispielsweise einem Service weitere Hosts hinzuzufügen oder die geerbte Einstellung wieder „auf Null“ zu setzen.

Bisher konnte man ein Objekt immer nur von einem Template ableiten, wodurch in manchen Installationen die Übersicht etwas gelitten hat. Nagios 3 führt eine mehrfache Vererbung von Templates ein (siehe Abb. 4). Zusammen mit der Option, die sogenannten „Extended Infos“ direkt beim Host beziehungsweise Service zu definieren, bietet es dadurch wieder großes Einsparpotenzial. Für Links, Bilder et cetera im Web-Frontend muss man nun nicht mehr weitere Objekte parallel zu Host und Services definieren – sie lassen sich über mehrere Templates vererben.

Schließlich kam noch für große Installationen eine Einstellung hinzu, die gewisse Verhaltensmuster von Nagios bezüglich Speicherverwaltung und Erzeugen neuer Prozesse verändert. Ein Teil davon [j] war schon in Nagios 2 vorhanden, nur musste man dazu die Einstellung direkt im Quellcode treffen. Nun kann dies über die Konfigurationsdatei erfolgen.

iX-Wertung

⊕ Open Source, keine Lizenzkosten

⊕ modularer Aufbau, Erweiterbarkeit

⊕ große (deutsche) Community, viele Erweiterungen verfügbar

⊖ mächtige Konfigurationsdateien erschweren den Einstieg

Fazit

Da die Änderungen am Nagios-Daemon [k] für viele Installationen wichtig und nötig sind, hat sich Ethan Galstadt entschlossen, das neue Outfit des Web-Frontends auf die Version 4 zu verschieben. In den ebenfalls oft kritisierten Konfigurationsdateien schufen die Entwickler weitere Einstellungsmöglichkeiten. Sie vereinfachen das Entstehen eines grafischen Konfigurationswerkzeugs nicht – im Gegenteil: Sie schaffen noch mehr Möglichkeiten, die solch ein Tool nur schwer abbilden kann. Nagios 3 ist auf jeden Fall ein großer Schritt nach vorne – für alte Nagios-Hasen genauso wie für -Interessierte, denen die vollständig überarbeitete und neu gestaltete Dokumentation den Einstieg wesentlich erleichtern sollte. Wer trotzdem noch Hilfe braucht, kann sich gelegentlich auf dem deutschsprachigen Nagios-Portal [l] umsehen. (avr)

SVEN VELT

arbeitet seit 2002 als Consultant und Trainer für die Teamix GmbH in Nürnberg; Nagios zählt zu seinen Spezialgebieten.

Onlinequellen

[a] Nagios	www.nagios.org
[b] Nagios-Plug-ins	www.nagiosplugins.org
[c] Gnokii	www.gnokii.org
[d] scmxx	www.hendrik-sattler.de/scmxx/
[e] NRPE	www.nagios.org/download/#addons
[f] NDOUtils	www.nagios.org/download/#ndoutils
[g] PNP	www.ederdrom.de/pnp/de/start
[h] NagiosGrapher	www.nagiosexchange.org/NagiosGrapher.84.0.html
[i] PerfParse	perfparse.sf.net
[j] Großinstallation	nagios.sf.net/docs/3_0/largeinstalltweaks.html
[k] Changelog	nagios.sf.net/docs/3_0/whatsnew.html
[l] Nagios-Portal	www.nagios-portal.de



Rapid Application Development mit Xdev 2

Instantkaffee

Bernhard Steppan

Rapid-Application-Development-Tools spielen im Java-Sektor bislang keine bedeutende Rolle. Die Firma Xdev will das mit ihrem gleichnamigen Werkzeug ändern. Es soll die Entwicklung von Java-Anwendungen vereinfachen und beschleunigen.

Das Entwickeln von Java-Anwendungen steht besonders bei Neulingen nicht gerade in dem Ruf, besonders einfach zu sein. Schuld an dieser Einschätzung tragen nicht nur die Programmiersprache und ihre Bibliotheken, sondern auch die Entwicklungsumgebungen. Auf professionelle Anwender zugeschnittene Werkzeuge wie Eclipse oder Netbeans überfordern manchen Einsteiger mit ihrer Vielzahl an Einstell- und Konfigurationsoptionen.

Xdev 2 der kalifornischen Firma Xdev, eine sogenannte RAD-Umgebung (Rapid Application Development), soll Abhilfe schaffen. Laut Hersteller ist sein Werkzeug die „weltweit einfachste Entwicklungsumgebung“, mit der man „Java-Anwendungen in absoluter Rekordzeit“ entwickeln könne. Das Produkt gibt es als Professional und Enterprise Edition (Einzelplatzlizenz). Weiterhin existieren ein Teamserver für die Arbeit mit mehreren Entwicklern und eine Spezialversion für die Datenbank Caché Objects. Xdev ist für Windows, Linux, Mac OS X und Solaris erhältlich. Als Testversion stand die Windows-Ausprägung der Enterprise Edition zur Verfügung.

Bei der Installation muss man die gewünschte Java-Laufzeitumgebung auswählen, wenn mehrere JDKs oder JREs auf dem System liegen. Der Installer suchte sich auf dem Testrechner nicht die neueste, sondern eine ältere Java-5-Release aus. Xdev wird mit einem USB-Kopierschutzstecker ausgeliefert, den Windows automatisch erkennt. Unter Linux und Mac OS X muss man einen Treiber installieren. Nachdem der USB-Stick erkannt und die Seriennummer eingegeben ist, lässt sich das Werkzeug starten.

Es präsentiert sich mit einer aufgeräumten Oberfläche. Im oberen Teil befinden sich Menü und Werkzeugleiste. Auf der linken Seite liegt eine Komponentenpalette, während die rechte dem Projektmanagement und den Komponenteneigenschaften vorbehalten ist. In der mittig angeordneten Arbeitsoberfläche kann der Anwender zwischen GUI-Builder und Code-Editor wechseln. Alle Fenster lassen sich umarrangieren. Registerreiter dienen zum schnellen Zugriff auf häufig benötigte Fenster.

In letzter Minute

Die Version 2.3.1 erreichte *iX* kurz vor Redaktionsschluss. Ein Kurztest ergab, dass Xdev einige Fehler beseitigt hat. Insbesondere der Menüeditor funktioniert deutlich besser. Andere Fehler wie die Onlinehilfe, die sich nicht aufrufen lässt, und einige der erwähnten Einschränkungen (Programmiersprache nicht konform zum Java-Standard) bestehen weiterhin. Nach eigenen Angaben arbeitet der Hersteller an einer Version, die es erlauben soll, Java-Sources zu exportieren. In Zukunft will man das Xdev-Framework offenlegen sowie einen neuen Texteditor zur Verfügung stellen.

Entwickeln mit grafischer Hilfe

Wie bei derartigen Werkzeugen üblich, verläuft das Entwickeln einer Anwendung top-down, also von der Arbeitsoberfläche aus. Nach dem Start ist demzufolge der GUI-Builder namens Guinea aktiviert, der wie ein Grafik- oder DTP-Werkzeug aussieht. Es gibt zwei Bearbeitungsmodi: Absolute (pixelgenaue) Positionierung von GUI-Komponenten ohne Layout-Manager sowie relatives Ausrichten mit Layout-Manager.

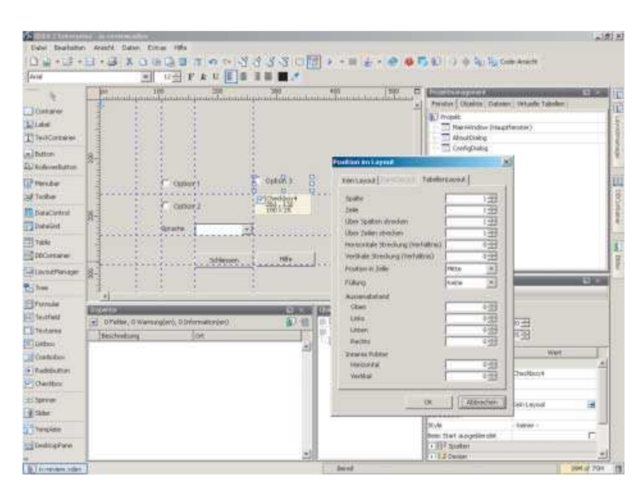
Mit Linealen und Hilfslinien platziert der Entwickler GUI-Komponenten an der gewünschten Stelle (absolute Positionierung). Ärgerlich ist, dass einmal aufgezogene Hilfslinien bei allen Dialogen und Fenstern automatisch an derselben Stelle erscheinen, auch wenn man sie dort gar nicht benötigt. Zudem docken die GUI-Komponenten nicht immer an den Linien an, was diese teilweise entwertet. Aber für die bevorzugte Methode beim Erstellen von Java-Oberflächen nützen diese Hilfsmittel sowieso nichts, arbeitet der Entwickler üblicherweise doch mit speziellen Java-Layouts und positioniert die Elemente relativ.

Guinea unterstützt dieses Vorgehen jedoch nur begrenzt. Von den in Java zur Verfügung gestellten Layouts bietet er nur zwei Varianten an: Rand- (Border) und Tabellenlayout (GridBag). Schaltet man zwischen den Layout hin und her, ändert sich am Modus des

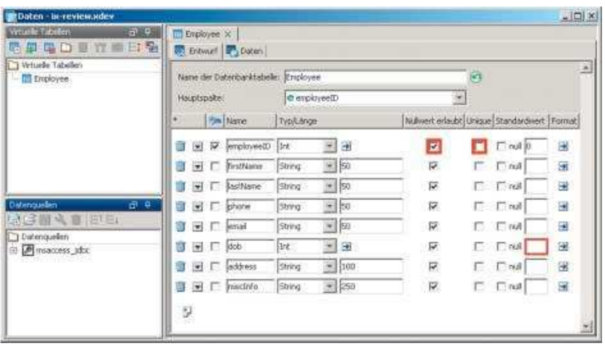
GUI-Builders wenig. Im Vergleich zu anderen Java-GUI-Buildern erweist sich die Layout-Bearbeitung in Guinea als umständlich und wenig intuitiv (Abb. 1).

Wer denkt, er könne per Drag & Drop seine Komponenten in das Raster eines Tabellenlayouts fallen lassen, hat sich getäuscht. Man muss viel tippen, um einen Dialog mit einem komplexen Tabellenlayout zu gestalten. Dass Guinea im Gegensatz zu manchem konkurrierenden GUI-Builder in Tabellen keine Life-Daten anzeigen kann, ist ein weiteres Manko. Die datensensitiven Komponenten, die Xdev zur Verfügung stellt und die an Borlands DbSwing-Komponenten erinnern, lösen einen Teil der Herstellerversprechen ein: Mit ihnen kann auch ein Einsteiger relativ leicht Datenbankanwendungen entwickeln.

Dreh- und Angelpunkt ist hierbei die Datenbankanbindung mit sogenannten virtuellen Tabellen, die als Zwischenspeicher für Datensätze fungieren. Über einen Dateneditor lassen sich die Schemata von Datenbanken einlesen, Beziehungen visualisieren und die Teile, die der Editor für die Anwendung benötigt, in virtuellen Tabellen ablegen (Abb. 2). Datenbankabfragen speichert Xdev ebenfalls in virtuellen Tabellen. Im GUI-Builder gibt man per Dateneditor die Tabelle an, deren Daten in einer GUI-Komponente erscheinen sollen.



Der GUI-Builder funktioniert wie ein DTP-Programm. Freies Positionieren ohne Einsatz des Layout-Managers klappt sehr gut, während die Unterstützung für den Layout-Manager zu wünschen übrig lässt (Abb. 1).



Virtuelle Tabellen sind die Tore zu den Datenbanken. Diese Zwischenspeicher legt der Entwickler samt der zugehörigen Datenquellen im Dateneditor an (Abb. 2).

Viele Fehler trüben den Genuss

Für die Entwicklung von Menüs ist nicht der GUI-Builder, sondern ein spezieller Editor zuständig. Leider produziert er eine Reihe von Fehlern: Ein Doppelklick auf einen Menüeintrag tauschte die Bezeichnung des Menüs mit der Beschriftung aus. Heißt ein Menü *FileMenu* und trägt die Beschriftung *Datei*, so wird nach dem Doppelklick unsinnigerweise der Bezeichner *FileMenu* als Beschriftung eingesetzt. Die Eingabe von Tastenkombinationen kann ebenfalls schwierig sein, da Xdev sich partout weigerte, deutsche Umlaute anzunehmen.

Für die Webentwicklung bietet Xdev ausschließlich Applets als Client-Technik an. Servlets beziehungsweise Webanwendungen mit Java Server Pages oder gar komplizierte Webapplikationen, die auf Frameworks wie Struts oder Java Server Faces basieren, lassen sich weder entwickeln noch importieren. Dazu fehlen sowohl die entsprechenden Editoren als auch die passende Laufzeit- sowie Testumgebung. Mit Java-GUIs, die auf die auf dem Eclipse-Framework SWT oder der Rich Client Platform basieren, kann Xdev ebenfalls nichts anfangen.

Überblick über die angelegten Fenster, Objekte, Dateien und virtuellen Tabellen verschafft die Projektverwaltung. Den Code, den das System für diese Ressourcen erzeugt, bekommt man niemals vollständig zu Gesicht. Nur auf einen kleinen Teil hat der Entwickler über den Code-Editor Zugriff. Bei Letzterem handelt es sich nicht um einen Texteditor im üblichen Sinne. Er beherrscht zwei Modi, die Block- und die Baumdarstellung des Codes. Die Sprache, mit der das Programm entwickelt werden soll, ist einstellbar. Das überrascht, erwartet man doch von einer Entwicklungsumgebung, die sich als „Rapid Application Development IDE für Java" bezeichnet, dass man Java-Code eingeben kann.

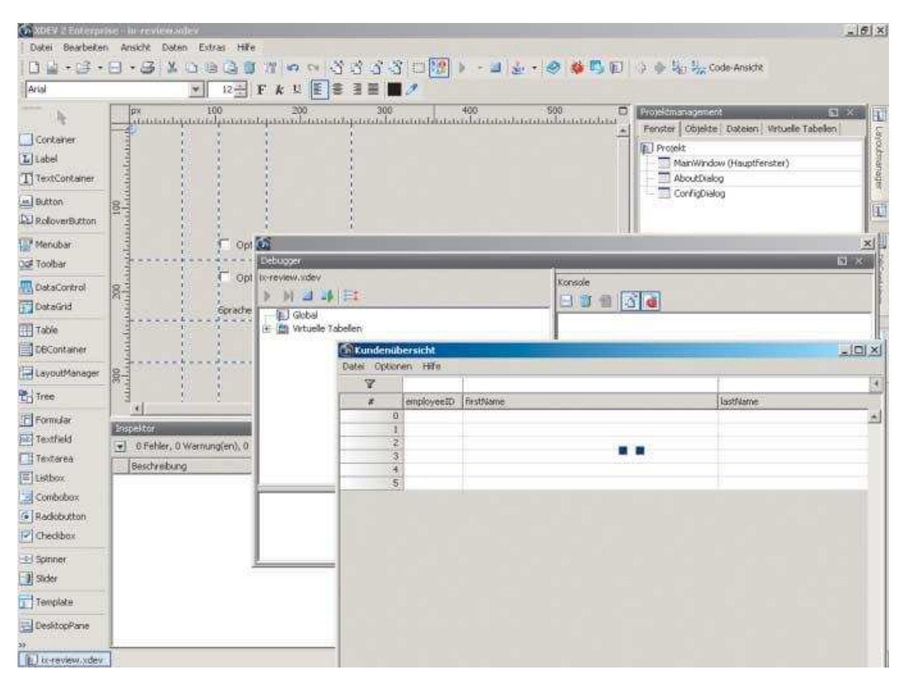
Der Editor beherrscht jedoch Dialekte wie Xdev Object Script oder Xdev Basic, ja sogar eine spezielle Sprachausprägung mit deutschen Schlüsselwörtern (Xdev NLS) – nur nicht Java. Das mag zunächst nicht stören, weil man sich davon eine einfachere Programmierung im Vergleich zu Java erhofft. Eher ist allerdings das Gegenteil der Fall, der Java-Entwickler steht plötzlich vor neuen Fragen: Wie ruft man zum Beispiel innerhalb eines Programms einen Dialog auf? Nicht, indem man wie bei objektorientierten Sprachen üblich ein neues Objekt einer bestehenden Dialogklasse erzeugt, sondern durch *Xdev CallWindow* gefolgt vom Namen einer Java-Klasse.

Die Frage nach dem Nutzen

Da einige Programmaufrufe der Java-Syntax ähneln, entsteht schnell ein Kauderwelsch, das nur Insider durchblicken dürften. Selbst wenn es eine Exportmöglichkeit für den Quelltext gäbe, ließen sich solche Programme nicht in anderen Entwicklungsumgebungen ausführen. Man fragt sich angesichts solcher Beschränkungen, wo nun die entscheidenden Vorteile liegen sollen, denn auch der Einsteiger ohne Java-Kenntnisse profitiert nicht unbedingt davon. Er kann beispielsweise nicht in der Java-Literatur nachschlagen, wenn er mit seinem Programm nicht weiterkommt. Das Begleitheft mit nicht einmal 20 Seiten und die Onlinehilfe, die sich von der IDE nicht aufrufen ließ (Abb. 3), dürfte ihn kaum weiterbringen.



Wie alle externen Programme ließ sich die Onlinehilfe wegen eines Verknüpfungsproblems nicht aufrufen (Abb. 3).



Die Programmvorschau im Testmodus funktionierte nicht einwandfrei. Der Debugger kann bei diesen und anderen Problemen nur wenig helfen (Abb. 4).

Neben der fehlenden Dokumentation bringen einen unerwartete Fehler immer wieder aus dem Tritt. Ein Beispiel liefert der Blockmodus des Code-Editors. Oft positionierte er den Cursor *vor* dem Zeilenanfang. In diesem Fall ist die Tastatursteuerung blockiert. Es hilft hier nur, den Cursor per Mausklick wieder an eine gültige Position zu setzen.

Xdev verfügt über einen Testmodus. Das entwickelte Programm lässt sich im Debugger ausführen. Allerdings sollte man den nicht mit seinen Pendants in Java-Entwicklungsumgebungen vergleichen. Er verfügt über weit weniger Funktionen. Beispielsweise ist es nicht möglich, Breakpoints in Bibliotheken oder außerhalb des sichtbaren Code-Rahmens zu setzen. Da praktisch der gesamte Code unsichtbar bleibt, stellt sich die Frage, wie man sein Programm genau untersuchen soll. Während des Tests kam es beispielsweise oftmals zu Fehlern bei der Datenbankverbindung und beim Aufbau des Hauptfensters (Abb. 4). Beide Fehler konnte der Debugger nicht eingrenzen oder gar beheben. Aus dem Programmcode erzeugt Xdev eine ausführbare Datei, die unter Windows die Endung *exe* besitzt. Sie enthält ein gepacktes Startprogramm und einige Bibliotheken. Das Programm besteht laut Hersteller aus proprietärem Bytecode, den eine Xdev-API zunächst interpretiert und der dann in einer Java-Laufzeitumgebung ausgeführt wird. Der Ressourcenbedarf der integrierten Entwicklungsumgebung bleibt anfangs erstaunlich gering. Auf einem PC mit 1 GHz Taktfrequenz und 512 MByte Hauptspeicher läuft die Anwendung flüssig. Mit zunehmender Entwicklungsdauer nimmt der Speicherhunger der Umgebung zu und kann bis zu 320 MByte erreichen.

Fazit

Die Werbebotschaft, mit Xdev 2 könne man zu keiner Zeit an Grenzen stoßen und Anwendungen in Rekordtempo entwickeln, ist angesichts der vielen Fehler und der starren Programmkonzeption nicht nachvollziehbar. Marketing und Werbung für das Produkt erscheinen auf der Firmenwebsite etwas diffus. Unklar bleibt, ob Xdev eine RAD IDE für die Sprache Java anbieten oder proprietäre Programme für die Java-Laufzeitumgebung erzeugen möchte. Weder von der Qualität noch vom Konzept her ist die Umgebung mit Java-IDEs wie Eclipse oder Netbeans vergleichbar. Mit Xdev erzeugte Programme lassen sich weder mit anderen Java-IDEs übersetzen noch basieren sie auf offenen Standards.

Neben diesen elementaren Einschränkungen schrecken vor allem die vielen Bugs nachhaltig ab. Auch führt die derzeitige Versionsnummer in die Irre: Das Produkt befindet sich gefühlt auf dem Entwicklungsstand 1.0. Trotzdem liegt im grundsätzlichen Konzept Potenzial. Und wer Einsteigern die Programmierung erleichtern will, verdient Vorschusslorbeeren. Doch sollte der Anbieter seinem Werkzeug Zeit geben, die notwendige Reife zu erlangen. Vielleicht präsentiert sich die Angelegenheit in einem Jahr wesentlich entspannter (siehe Kasten „In letzter Minute“). (jd)

BERNHARD STEPPAN

arbeitet als Softwareentwickler und freier Autor in Bad Homburg.

iX-Wertung

⊕ einfache Datenbankanbindung

⊕ datensensitive GUI-Komponenten

⊕ weitgehend visuelle Programmierung

⊖ viele Fehler

⊖ nicht konform zur Java-Sprache

⊖ unzureichende Dokumentation

Lieferumfang und Preise

Xdev 2, 2.3 Enterprise Edition

Speicherbedarf	256 MByte RAM, 100 MByte Platte
Hardware	750 MHz Pentium-Prozessor
Betriebssystem	Windows, Linux, Mac OS X, Solaris
Preis	1700 Euro (Einzellizenz)
Anbieter	Xdev, www.xdev-software.de



Amazon verkauft Rechenleistung mit Elastic Compute Cloud

Mehr als einer

Nathanael Obermayer

Ohne großes Aufsehen hat die bekannte Onlinebuchhandlung Amazon ihr Portfolio auf IT-Dienstleistungen ausgedehnt und bietet Kunden mit „Elastic Compute Cloud" Rechenleistung zum Kauf an.

Die Fähigkeit, mehrere virtuelle Rechnerinstanzen laufen zu lassen, bringen die Linux-Distributionen heute in Form der Software Xen von Haus aus mit. Aus großen Rechenzentren ist Virtualisierung seit Längerem nicht mehr wegzudenken, so auch nicht im RZ von Amazon. Mitte 2006 begann die Onlinebuchhandlung, interessierten Beta-Testern eigene virtuelle Rechnerinstanzen bereitzustellen. Im Amazon-Jargon laufen die Systeme in der „Elastic Compute Cloud", der Service heißt deshalb kurz „EC2". Die Abrechnung erfolgt in US-$ und stundenweise, der Anwender kann jederzeit die gerade benötigte Anzahl virtueller Rechner starten, zahlt aber nur für die tatsächlich genutzte Zeit und den anfallenden Datenverkehr.

Gerade Webanwendungen kämpfen häufig mit Lastspitzen, während zu anderen Zeiten die Server sozusagen Däumchen drehen. Daher ist es nicht verwunderlich, dass viele der sogenannten Web-2.0-Startups sich sofort für das Amazon-Angebot begeisterten, denn sie sparen die Anschaffungskosten für eigene Server und können im Falle eines plötzlichen Erfolgs einfach zusätzliche Instanzen starten. Bis in den Herbst 2007 hinein bot Amazon die Dienstleistung nur in einer geschlossenen Beta-Tester-Gruppe an. Nach der Registrierung auf Amazons Website mussten Entwickler wegen der großen Nachfrage oft wochenlang auf einen Account warten. Seit Mitte Oktober 2007 ist das Angebot öffentlich zugänglich, obwohl Amazon den Service weiterhin als Beta bezeichnet.

Virtuelle Maschinen mit angepasstem Kernel

Im Hintergrund setzt Amazon ein modifiziertes Xen in Version 3.0.2 ein. Direkt damit in Berührung kommt der Anwender jedoch nicht. Amazon bietet eigene Kommandozeilen-Werkzeuge an, die die Xen-Details vor dem Benutzer verstecken. Um eine Rechnerinstanz zu starten, muss der Anwender ein sogenanntes „Amazon Machine Image" (AMI) auswählen. Er kann dann durch ein Kommando eine Rechnerinstanz mit dem Image booten. Es umfasst dabei, ähnlich wie bei einem Festplatten-Image, jeweils eine komplette Linux-Installation ohne eigenen Kernel. Amazon setzt einen speziell angepassten der 2.6-Reihe ein, den der Anwender nicht austauschen kann.

Erfreulicherweise stellt Amazon die Kernel-Sourcen online zur Verfügung (siehe Onlinequellen [a]), */proc/config.gz* liefert zur Laufzeit die vollständige Konfiguration. Der Anwender kann eigene Module kompilieren, wozu er *gcc 4.0* einsetzen muss. Einige beliebte Grid-Lösungen brauchen jedoch einen eigenen angepassten Kernel und laufen auf dem bereitgestellten nicht. Viele rechenintensive wissenschaftliche Anwendungen können die EC2-Plattform daher nicht nutzen. Über *qemu* gelang es, Windows in verschiedenen Versionen laufen zu lassen, was eher als

iX-TRACT

- Mit EC2 bietet die Onlinebuchhandlung Amazon Rechenzeit zur Miete an.
- In der „Elastic Compute Cloud" laufen Systeme mit angepasstem Kernel.
- Solche Amazon Machine Images können Benutzer auch selbst erstellen.
- EC2 befindet sich noch im Beta-Stadium.

Hack denn als tatsächliche Option gelten dürfte.

Eine gestartete Instanz kann der Anwender aus der Ferne kontrollieren. Er darf die Instanz neu starten und die dynamisch zugewiesene IP-Adresse abfragen. Statische Adressen unterstützt EC2 nicht. Beim Start lässt sich die Rechnerkonfiguration festlegen, sie ist jedoch in der Ausstattung beschränkt. Er kann nur zwischen drei Varianten auswählen, die nicht anpassbar sind.

Zusätzlicher Hauptspeicher oder weitere virtuelle Festplatten sind nicht konfigurierbar. Als Maßeinheit für Rechenkraft setzt Amazon eine eigene „EC2 Compute Unit“ ein. Laut deren Angaben entspricht eine Einheit in etwa einem 1 bis 1,2 GHz schnellen Opteron- oder Xeon-Prozessor. Bis Mitte Oktober war nur die inzwischen „Small Instance“ getaufte Konfiguration verfügbar. Sie umfasst eine 32-bittige EC2-Compute-Einheit mit 1,7 GByte Memory sowie 160 GByte sogenanntem Instanzspeicher (quasi eine virtuelle Festplatte). Hinzugekommen sind inzwischen die 64-Bit-Konfigurationen „Large“ und „Extra Large“ mit vier respektive acht CPU-Kernen und je zwei EC2-Compute-Einheiten. Als Hauptspeicher stehen 7,5 beziehungsweise 16 GByte zur Verfügung. Der Instanzspeicher umfasst 850 respektive 1700 GByte. Außerdem unterscheiden sich die Konfigurationen in der I/O-Geschwindigkeit. Amazon spricht von „moderater“ und „hoher“ Geschwindigkeit, über die eingesetzte Technik gibt es keine offizielle Verlautbarung.

Technisch entspricht der Speicher zurzeit in etwa einer SATA-Platte. Eine Garantie, dass dies so bleibt, gibt Amazon ausdrücklich nicht. Es spricht nie von Festplatten, sondern benutzt ausschließlich den Begriff Instanzspeicher, wohl um den Unterschied zu einer echten Festplatte zu betonen: Denn nach einem Absturz oder dem Beenden einer Rechnerinstanz verschwindet der gesamte Inhalt des Instanzspeichers. Zwar überleben die dort hinterlegten Daten den geplanten Neustart eines Rechners, aber wichtige Informationen muss der Anwender dauerhaft speichern. Amazon verweist auf seinen eigenen „Simple Storage Service“ (S3), einen dezentralen hochverfügbaren Speicher, den der Kunde über Webservices ansprechen, den er jedoch nicht so ohne Weiteres per *mount* einbinden kann.

S3-Service nur mit Amazons Machine Image

Ähnlich wie bei EC2 bezahlt der Anwender für den S3-Service keine Grundgebühr. Der Preis beträgt 0,15 US-$ pro Gigabyte im Monat, hinzu kommen weitere Cent-Beträge für die Datenübertragung. Finanziell und technisch sind die Webdienste von Amazon geschickt miteinander verbunden. Ein AMI muss bei S3 hinterlegt sein, um den Dienst starten zu können; zusätzliche Kosten für den Datentransport zwischen zwischen EC2-Instanzen und S3 fallen nicht an. Bei der Anmeldung muss sich der EC2-Beta-Tester zugleich für S3 anmelden.

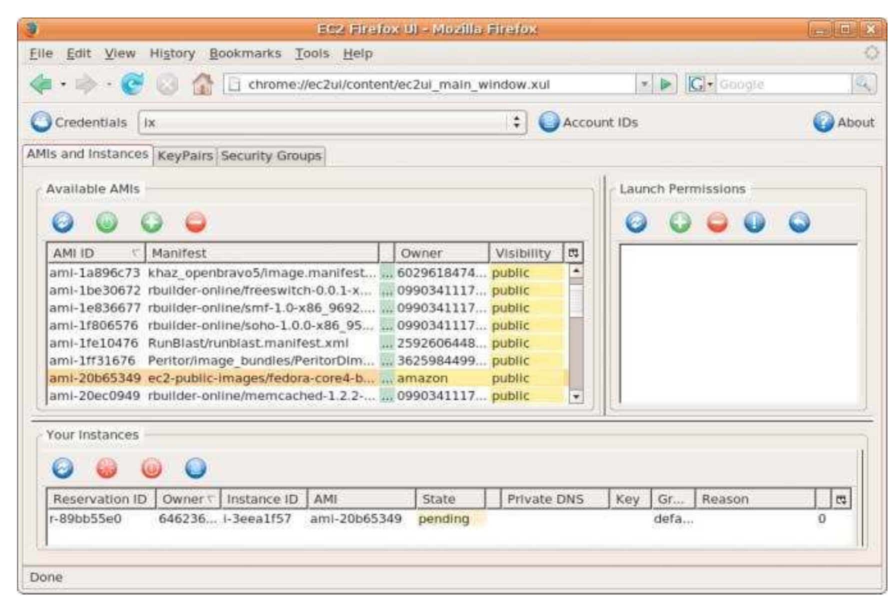
Um einen Rechnerausfall zu überstehen, sollte der Anwender alle gespeicherten Daten in regelmäßigen Abständen in das S3-System kopieren. Inzwischen gibt es dafür einige Werkzeuge von Drittanbietern, beispielsweise den User-Space-Filesystemtreiber *s3infidisk*, der S3-Speicher per *mount* einhängen kann. Will jemand den Rechner als einfachen Datei- oder Webserver einsetzen, kann das eine Lösung für dauerhaften Speicher sein. Spätestens beim Einsatz einer Datenbank müssen jedoch andere Mechanismen her. Viele Anwender setzen auf Datenbank-Systeme mit Failover und replizieren den Datenbestand. Inzwischen bieten einige Startups fertig konfigurierte AMIs für die populären Open-Source-Datenbanken an und ersparen dem Anwender zusätzlichen Konfigurationsaufwand [b, c]. Amazon unterstützt durch einen eigenen Abrechnungsmechanismus die Anbieter solcher „Bezahl-AMIs“ und stellt dem Anwender automatisch einen zusätzlichen Betrag pro Betriebsstunde in Rechnung (siehe „Preisliste“).

Vorgefertigte Images mit Fedora Core

Amazon selbst bietet eine kleine Auswahl eigener AMIs an, die der Anwender direkt ohne weitere zusätzliche Kosten starten kann. Die Images von Amazon basieren auf der Linux-Distribution Fedora Core. Wer auf eine andere Distribution ausweichen möchte, ist aufs Selbermachen angewiesen. Anfang November 2007 hatten Amazon und Red Hat eine Zusammenarbeit angekündigt, es gibt jedoch noch keine öffentlich verfügbaren AMIs.

Um AMIs starten zu können, muss der Anwender die EC2-API-Tools installieren. Die Tools steuern und überwachen per SOAP (Simple Object Access Protocol) den Lebenszyklus der Instanzen. Intern nutzt Amazon Java in der Version 1.5, das ebenfalls installiert sein muss. Zusätzlich gibt es inzwischen ein bedienerfreundliches Firefox-Plug-in zum Steuern der eigenen virtuellen Maschinen, das Amazon zum Herunterladen bereitstellt [d].

Den eigentliche Zugriff der Werkzeuge hat Amazon über ein X509-Zertifikat gesichert. Der Anwender kann entweder ein eigenes hochladen oder sich ein neues generieren lassen. Amazon bietet einen kurzen Leitfaden für



Lange Liste: Bei der Nutzung von Elastic Compute Cloud geht es nicht nur ums Rechnen. Eine lange Liste vorgefertigter Images für virtuelle Maschinen steht zur Verfügung (Abb. 1).

die ersten Schritte an, der die Zertifikats-Erstellung und Tool-Konfiguration umfasst [e]. Nach der Einrichtung erhält man eine Liste der verfügbaren Amazon-AMIs durch:

```
ec2-describe-images -o amazon
```

Das Starten einer Instanz erfolgt durch

```
ec2-run-instances AMI-NAME -k keypair
```

Über einen eleganten Mechanismus kann der Anwender beim Starten einer Instanz Schlüssel-Werte-Paare übergeben, die er aus dem laufenden System abfragen kann. Der Parameter *–k* erlaubt die Übergabe eines Zertifikats, um den SSH-Zugang zu sichern.

Nach dem Startbefehl erhält der Anwender eine eindeutige Instanz-Nummer. Mit dem Befehl *ec2-describe-instances* und der Nummer kann der Anwender den Start seines virtuellen Rechners verfolgen. Mittels *ec2-terminate-instances* und der Instanz-Nummer kann er den Betrieb wieder beenden.

Beim Starten einer Instanz ordnet EC2 sie immer einer Sicherheitsgruppe zu. Sofern vom Anwender nicht anders angegeben, gilt die Gruppe „default“. Für jede einzelne kann der Anwender eigene Firewall-Regeln konfigurieren. Ohne eine Änderung daran sind gar keine Ports geöffnet. Für SSH-Zugriff muss mit

```
ec2-authorize default -p 22
```

der Port 22 für die Gruppe „default“ freigeschaltet sein. Der Anwender kann Zugriff auf bestimmte Ports nur anderen EC2-Instanzen erlauben, den Internetverkehr aber ausschließen. Die EC2-Maschinen sind hinter einem 1:1-NAT versteckt, besitzen eine öffentliche und eine interne IP-Adresse.

Zum Erzeugen eigener AMI, dem Abbild einer virtuellen Maschine, stellt Amazon Werkzeuge als Bash- und Ruby-Skripte zum Download bereit. Die Hilfsmittel erstellen aus einem laufenden Linux System heraus ein AMI. Der Anwender kann sein System nach seinen Wünschen anpassen und mit *ec2-bundle-vol* ein neues startbares AMI erzeugen. EC2 verschlüsselt das erstellte Image automatisch und signiert es, der Anwender benötigt also auch hier seine Zertifikate.

Den Upload eines erstellten Image zu S3 kann der Anwender ebenso direkt über die Kommandozeile durchführen, nur muss er die Datei für den Einsatz als AMI anschließend aktivieren. Er kann über ein simples Rechte-System bestimmen, wer das Image sehen und starten kann. Auf diese Weise kann er ein eigenes allen anderen Benutzern bereitstellen. Bisher hat die Community über 200 solcher Public Images erstellt, die jedem Anwender zur Verfügung stehen. Leider bietet Amazon keinen übersichtlichen Katalog der vorhandenen an. Es gibt jedoch ein vorbereitetes HTML-Template, das man im Forum veröffentlichen kann. Den AMI-Anbieter überprüft Amazon nicht; wer ein fremdes AMI einsetzt, muss sich der Sicherheitsrisiken bewusst sein.

Fazit

Während der mehrere Monate dauernden Erprobungen liefen die Instanzen anstandslos durch, in der Hinsicht wirkt der Dienst absolut verlässlich. Die Kommandozeilen-Werkzeuge leiden jedoch teilweise noch unter Kinderkrankheiten. Selbst beim einfachen Durcharbeiten des „Getting Started Guide“ trifft der Anwender noch auf Fehler. Bei Schwierigkeiten findet er im offiziellen Forum [f] jedoch fast immer schnell Hilfe, häufig direkt von Amazon-Mitarbeitern. Amazon selber rät vom Produktiv-Einsatz bisher ausdrücklich ab, deshalb erfolgt keine *iX*-Wertung. Der offizielle Solution Catalog dokumentiert allerdings, wie häufig der Rat in den Wind geschlagen wird [g]. Amazon gibt bisher keine Verfügbarkeitsgarantie. Da das Unternehmen für den S3-Service erst vor Kurzem Service Level Agreements eingeführt hat, könnte das bald mit EC2 geschehen.

Das Fehlen einer dauerhaften Speichermöglichkeit in Form einer direkt mountbaren Festplatte ist wohl das größte Manko des EC2-Angebots. Für viele Aufgaben muss der Anwender zu komplizierten Workarounds wie gespiegelten Datenbanken greifen, die bei klassischem Hosting nicht notwendig sind. Eine LAMP-Anwendung ist auf einem normalen VServer einfacher zu installieren. Viele Startups nehmen die Nachteile des Instanzspeichers in Kauf, um bei Bedarf einfach und billig skalieren zu können. Gerade im Ruby-on-Rails-Umfeld gibt es daher inzwischen viele Tipps und Best Practices zur Konfiguration eigener AMIs. Von Haus aus bietet Amazon keine Unterstützung, um lastabhängig automatisch weitere Instanzen zu starten. Load-Balancing-Lösungen muss der Anwender ebenso selber konfigurieren. Startups wie Rightscale [c] und Weoceo [h] haben diese Lücke aber bereits geschlossen.

Klassische rechenintensive Aufgaben aus dem wissenschaftlichen Bereich kommen teilweise mit dem festgelegten Kernel nicht zurecht. Für Batch-Prozesse, beispielsweise zum Konvertieren von Videodateien, eignet sich EC2 hingegen optimal [i]. Das schnelle Auftauchen direkter Konkurrenten wie Flexiscale [j] spricht für das wirtschaftliche Potenzial des Amazon-Angebots. (rh)

NATHANAEL OBERMAYER

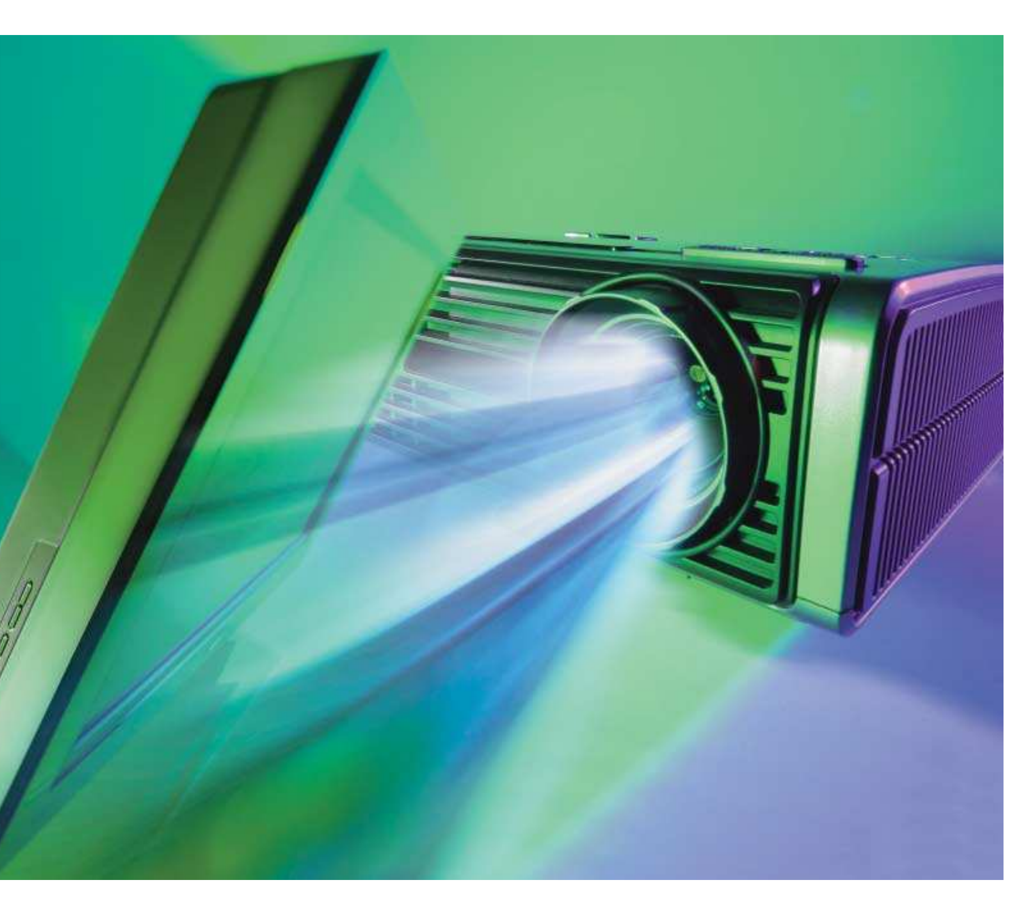
arbeitet als Geschäftsführer der Codecentrated Limited und unterstützt Unternehmen aus der Telekommunikations- und Finanzbranche bei der Entwicklung verteilter Anwendungen.

Preisliste für EC2

Preis in US-$	Small	Large	Extra Large
pro angefangener Stunde	0,10	0,40	0,80
pro GByte eingehendem Traffic	0,10	0,10	0,10
pro ausgehendem GByte (erste 10 TByte)	0,18	0,18	0,18
pro ausgehendem GByte (nächste 40 TByte)	0,16	0,16	0,16
pro ausgehendem GByte (über 50 TByte)	0,13	0,13	0,13

Onlinequellen

[a] s3.amazonaws.com/ec2-downloads/linux-2.6.16-ec2.tgz
[b] www.elastra.com/
[c] rightscale.com/
[d] developer.amazonwebservices.com/connect/entry.jspa?externalID=609
[e] docs.amazonwebservices.com/AWSEC2/2007-08-29/GettingStartedGuide
[f] developer.amazonwebservices.com/connect/forum.jspa?forumID=30
[g] solutions.amazonwebservices.com/connect/kbcategory.jspa?categoryID=89
[h] weoceo.weogeo.com/
[i] open.blogs.nytimes.com/2007/11/01/self-service-prorated-super-computing-fun/?
[j] flexiscale.com/



Marktübersicht: Groß-Displays und Projektoren

Zurschausteller

Dieter Michel

Sei es, dass man etwas verkaufen oder bewerben will oder mehreren Leuten gleichzeitig Informationen vermitteln möchte – große Displays oder Projektoren helfen hier weiter. Aber nicht jedes Gerät ist für jeden Zweck gleichermaßen gut geeignet.

Moderne Präsentationsmedien sind häufig in den heutigen Geschäftsalltag integriert. Sei es bei Besprechungen und Meetings im Konferenzraum oder auf Messen, Tagungen oder Firmenveranstaltungen. Vor Ort beim Kunden ebenso wie als Informations- und Werbe-Displays etwa am Point-of-Sale (POS). Die verbreitetsten elektronischen Präsentationsmedien sind Groß-Displays und Projektoren, Letztere meist für die Aufprojektion, in Konferenzräumen auch in Form einer Rückprojektionsinstallation. Dieser Artikel soll klären, welche Geräte sich für welche Anwendung am besten eignen und welche bilderzeugende Technik man für den jeweiligen Einsatz sinnvollerweise wählt.

Bei der grundsätzlichen Entscheidung zwischen Display und Projektion spielen vor allem die Gesichtspunkte Bildgröße, Fremdlichteinfluss und Mobilität des Präsentationssystems eine Rolle. Werden große Bildflächen über 2,5 m Bilddiagonale benötigt, kommt praktisch ausschließlich die Projektion infrage, wobei man darauf achten sollte, dass der maximale Lichtstrom des Projektors angemessen dimensioniert ist. Groß-Displays gibt es heutzutage bis zu einer Diagonalen von etwas über 100 Zoll (entsprechend 2,54 m). Das sind aber schon recht große Systeme, die aufgrund ihres Preises von circa 70 000 € derzeit eher als Messe-Eyecatcher angemietet und seltener im normalen Konferenzraum installiert werden.

Projektoren sind Lichtventile

Die derzeit gängigsten Projektoren arbeiten mit drei verschiedenen bildgebenden Techniken: LCD, LCoS und DLP. Alle drei Verfahren lassen sich unter den Begriff „Lichtventil“ zusammenfassen, da sie den Lichtstrom einer konstant leuchtenden Projektionslampe steuern und zwar für jedes Bildpixel und jede Grundfarbe individuell.

LCD steht für Liquid Crystal Display und bezeichnet ein Projektionsverfahren, das ähnlich funktioniert wie ein normaler Computermonitor. Die Projektionslampe beleuchtet einen Prismenblock, in dem Interferenzfilter das Licht in drei Spektralbereiche – entsprechend den Grundfarben Rot, Grün und Blau – zerlegen, linear polarisieren und auf drei separate LCD-Panels lenken. Diese sind wesentlich kleiner als die eines Computermonitors, sie haben eine Bilddiagonale von nur zwei bis drei Zentimetern und lassen sich daher in kompakten Projektoren unterbringen. Wie das im Detail geschieht, erläutert der Artikel „Kristall und Spiegel“ in diesem Heft.

Alterung durch hohe Energie

Je nach Bauausführung ist die Zellenstruktur des LCD-Panels mit Dünnfilmtransistor mal mehr, mal weniger deutlich sichtbar. Bei deutlich ausgeprägter Sichtbarkeit spricht man vom sogenannten „Fliegengittereffekt“. Moderne Konstruktionen versuchen, mit einem Mikrolinsenraster das Licht der Projektionslampe auf die Mitte jeder Zelle zu fokussieren und so an der Transistorstruktur vorbeizuleiten. Das bringt mehr Lichtdurchsatz und lässt die Gitterstruktur in den Hintergrund treten.

Der Vorteil der LCD-Technik besteht darin, dass man über die Ansteuerspannung der Zellen und die Ausführung der Farbfilter eine gute Kontrolle

über die Helligkeitsabstufungen und die Farbwiedergabe hat. Für farbkritische Projektionen setzt man daher gern LCD-Projektoren ein.

Ein Nachteil ist, dass es sich bei den Flüssigkristallen um spezielle organische Verbindungen handelt. Sie befinden sich komplett im Lichtweg, das heißt, sämtliches Licht, das auf die Leinwand gelangt, muss zuvor auf einer relativ kleinen Querschnittsfläche von nur wenigen Quadratzentimetern durch die Flüssigkristallschicht hindurch. Die Lichtintensität ist an dieser Stelle also sehr hoch. Speziell im blauen Farbkanal, in dem die Photonen eine verhältnismäßig hohe Energie haben, kann es vorkommen, dass absorbierte Photonen so viel Energie auf das Molekül übertragen, dass sie es zerstören und unwirksam machen. Dadurch ist speziell das Panel für den Blaukanal Alterungserscheinungen ausgesetzt, die dazu führen, dass sich Durchlässigkeit und Sperrverhalten und mithin der Kontrast verschlechtern. Im Zusammenspiel mit den anderen Farbkanälen ergeben sich so zudem Farbverschiebungen, normalerweise in Richtung eines Gelbstichs. Für den Dauerbetrieb (etwa für Werbe-Displays) sind LCD-Projektoren demnach nicht so gut geeignet.

Auch im Normalbetrieb muss man damit rechnen, dass je nach täglicher Betriebsdauer nach einigen Jahren die Panels getauscht werden müssen. Letztendlich ist das eine kalkulatorische Frage, denn wenn die Panels bis zur nächsten Projektorgeneration beziehungsweise über die Abschreibungsperiode hinaus halten, nach der ohnehin Neuanschaffungen anstehen, ist dies in der Praxis bedeutungslos.

LCoS, Liquid Crystal on Silicon, ist eine Variante der LCD-Technik, die reflektiv arbeitet und daher die Transistoren hinter der Reflexionsschicht unterbringen kann. Da sie mithin nicht mehr im Lichtweg liegen, müssen die Transistoren bei hoher Panel-Auflösung nicht extrem klein werden. Deshalb eignet sich die LCoS-Technik gut für hochauflösende Displays. LCoS arbeitet mit einer Flüssigkristallschicht als Lichtmodulator, sodass bezüglich der Langzeitstabilität sinngemäß dasselbe gilt wie bei LCD-Panels.



- Groß-Displays oder Projektoren kommen als Präsentationsmedien in unterschiedlichen Bereichen zum Einsatz, beispielsweise in Konferenzräumen, auf Messen oder als Werbe-Displays am Point-of-Sale.
- Bei der Wahl zwischen Display und Projektion spielen diverse Faktoren eine Rolle, unter anderem die Bildgröße, der Fremdlichteinfluss oder die Mobilität des Präsentationssystems.
- Im Bereich der Projektoren unterscheidet man zwischen drei Verfahren für die Bildwiedergabe – LCD, LCoS und DLP –, die unterschiedliche Stärken haben.
- Für Groß-Bildschirme gibt es zwei Techniken – LCD und Plasma – die unterschiedlich funktionieren. Demzufolge sind sowohl die Vor- als auch die Nachteile anders gelagert.

Groß-Displays

Hersteller	LG Electronics	LG Electronics	Panasonic Deutschland	Panasonic Deutschland	Panasonic Deutschland	Panasonic Deutschland
Website	www.lge.com	www.lge.com	www.panasonic.de	www.panasonic.de	www.panasonic.de	www.panasonic.de
Produktname	Flatron M4710C	Flatron M5201C[1]	TH-50PF10EK	TH-58PH10EK	TH-65PF10EK	TH-103PF10EK (Großbild)
Varianten	–	M3202C, M3701C	TH-50PF10EK/ES	–	–	–
Preis (ohne MwSt.)	1470 €	3865 €	3176 €	3638 €	7058 €	63 529 €
Marktbereich	TFT-Flachbildschirme, Digital Signage, POS, POI	TFT-Flachbildschirme	AV-Installationen, Vermietung, Werbung, Digital Signage	AV-Installationen, Vermietung, Werbung, Digital Signage	AV-Installationen, Vermietung, Werbung, Digital Signage	AV-Installationen, Vermietung, Werbung, Digital Signage
Bildgeometrie						
native Auflösung	1366 × 768	1920 × 1080	1920 × 1080	1366 × 768	1920 × 1080	1920 × 1080
max. Signalauflösung (interpoliert)	1600 × 1200 bei 60 Hz (analog), 1280 × 1024 bei 60 Hz (digital)	1920 × 1200 bei 60 Hz (analog); 1280 × 1024 bei 60 Hz (digital)	k. A.	k. A.	k. A.	1920 × 1200
Seitenverhältnis (Bildgeometrie)	Diagonale: 47 Zoll (119,38 cm); aktive Fläche: 1039,69 × 584,82 mm, 16:9	Diagonale: 47 Zoll (132,08 cm); aktive Fläche: 1039,68 × 584,82 mm	Diagonale: 127 cm; effektiv: 110,6 × 62,2 cm	Diagonale: 147 cm; effektiv: 128,7 × 72,3 cm	Diagonale: 165 cm; effektiv: 143,4 × 80,7	Diagonale: 260 cm; effektiv: 226,9 × 127,7 cm
Funktionsprinzip	TFT-LCD	TFT-LCD	Plasma	Plasma	Plasma	Plasma
Anschlüsse						
Signaleingänge/-ausgänge	HDMI, RGBHV (15-Pin), S-V, C-V, Monitor: RGBHV	HDMI, RGBHV (15-Pin), S-V, C-V, Monitor: RGBHV	RGBHV (VGA Sub-D HD 15-polig), DVI-D, Komponenten-Video (alle Eingänge inkl. Audio); optional: div. Schnittstellen aufgrund des Slot-Konzepts	RGBHV (VGA Sub-D HD 15-polig), DVI-D, Komponenten-Video (alle Eingänge inkl. Audio); optional: div. Schnittstellen aufgrund des Slot-Konzepts	RGBHV (VGA Sub-D HD 15-polig), DVI-D, Komponenten-Video (alle Eingänge inkl. Audio); optional: div. Schnittstellen aufgrund des Slot-Konzepts	RGBHV (VGA Sub-D HD 15-polig), DVI-D, USB Host, Ausgang: optisch, (Eingänge inkl. Audio); optional: div. Schnittstellen aufgrund des Slot-Konzepts
Steuereingänge/-ausgänge	RS232C; Lautsprecher: 2 mal 10 W; VESA Plug & Play: DDC2B	RS232C	RS232C	RS232C	optional: div. Schnittstellen aufgrund des Slot-Konzepts	optional: div. Schnittstellen aufgrund des Slot-Konzepts
modulare Eingangsbestückung	k. A.	k. A.	diverse Eingangsmodule	diverse Eingangsmodule	diverse Eingangsmodule	diverse Eingangsmodule
HDCP an DVI	k. A.	k. A.	ja	ja	ja	ja
WLAN für Steuerzwecke	k. A.	nein	ja, optional über PCS oder WLAN-Board	ja, optional über PCS oder WLAN-Board	ja, optional über PCS oder WLAN-Board	ja, optional über PCS oder WLAN-Board
WLAN für Datenübertragung	k. A.	nein	ja, optional über PCS oder WLAN-Board	ja, optional über PCS oder WLAN-Board	ja, optional über PCS oder WLAN-Board	ja, optional über PCS oder WLAN-Board
Leistungsdaten						
max. Leuchtdichte	k. A.	k. A.	k. A.	k. A.	k. A.	k. A.
Fullscreen-Kontrast	800:1	800:1	k. A.	k. A.	k. A.	k. A.
Leistungsaufnahme (Betrieb/Eco/Standby)	Ein: <300 W; Standby: 2 W (RGB), 4 W (HDMI); Aus: 1 W	k. A.	595 W/1 W	630 W/1 W	725 W/1 W	1500 W/1 W
Ausstattung						
Farbmanagement	k. A.	k. A.	einstellbar	einstellbar	k. A.	einstellbar
Farbtemperatur	9300° K oder 6500° K	9300° K oder 6500° K	3200°, 6500°, 9300°, 11 300°	3200°, 6500°, 9300°, 11 300°	3200°, 6500°, 9300°, 11 300°	3200°, 6500°, 9300°, 11 300°
Farbbalance	einstellbar	einstellbar	Farbe und NTSC-Farbe	Farbe und NTSC-Farbe	Farbe und NTSC-Farbe	Farbe und NTSC-Farbe
6-Achsen-Farbmanagement (RGB/CMY)	RGB-Farben	RGB-Streifen	Weißabgleich RGB und Grauabgleich RGB	Weißabgleich RGB und Grauabgleich RGB	Weißabgleich RGB und Grauabgleich RGB	Weißabgleich RGB und Grauabgleich RGB
Film-Modus (manuell/automatisch)	manuell	k. A.	manuell (Cinema-Mode)	manuell (Cinema-Mode)	manuell (Cinema-Mode)	manuell (Cinema-Mode)
HD-kompatibel	ja	k. A.	ja	ja	ja	ja
Sonstiges						
Maße	Monitor: 1117,1 × 660,9 × 121 mm; Rahmenbreite: 29 mm rechts, und links 29 mm oben, 32 mm unten	Monitor: 1283,2×766,32×117,4 mm	1120 × 724 × 95 mm	1399 × 843 × 99 mm	1554 × 925 × 99 mm	2414 × 1421 × 129 mm
Gewicht	29 kg (netto), 32 kg (brutto)	52 kg (netto)	42 kg	54 kg	74 kg	220 kg
Lieferumfang	Netz-, VGA- und Audiokabel, Treiber und Handbuch auf CD, IR-Fernbedienung inkl. Batterien	k. A.	Netzkabel, Bedienungsanleitung, 2 Kabelbinder, Fernbedienung inkl. Batterien	Netzkabel, Bedienungsanleitung, 2 Kabelbinder, Fernbedienung inkl. Batterien	Netzkabel, Bedienungsanleitung, 2 Kabelbinder, Fernbedienung inkl. Batterien	Netzkabel, Bedienungsanleitung, 2 Kabelbinder, Fernbedienung inkl. Batterien
Besonderheiten			Bild-im-Bild	Bild-im-Bild	Bild-im-Bild	Bild-im-Bild

[1] Marktstart geplant für April 2008

Pioneer	Pioneer	Samsung Electronics	Samsung Electronics	Sharp Electronics (Europe)	Sharp Electronics (Europe)
www.pioneer.de	www.pioneer.de	www.samsung.de	www.samsung.de	www.sharp.de	www.sharp.de
Kuro PDP-LX508D	PDP-50MXE20	SyncMaster 570DX	PPM 50M6H	PN-525E	PN-G655E
Kuro PDP-LX5080 dito 60-Zoll-Geräte	PNG655RE: 17 490 €	32 bis 57 Zoll	42 bis 63 Zoll	–	PN-G655RE (für Dauerbetrieb im Hochformat)
4369 €	2853 €	9999 €	2199 €	6460 €	15 990 €
k. A.	k. A.	POS/POI	POS/POI	Digital Signage, Vermietung, AV-Installationen, Leitwarten	Digital Signage, Vermietung, AV-Installationen, Leitwarten
1920 × 1080	1366 × 768	1920 × 1080	1366 × 768	1920 × 1080 (Full HD)	1920 × 1080 (Full HD)
k. A.	k. A.	k. A.	k. A.	1920 × 1080 (Full HD)	1920 × 1080 (Full HD)
16:9	16:9	16:9	16:9	16:9, 52-Zoll-Bilddiagonale	16:9, 65-Zoll-Bilddiagonale
Plasma	Plasma	LCD-TFT	Plasma	LCD	LCD
HDMI, YUV, S-V, C-V, Euro-Scart, CI-Slot, PC-Eingang, über Videoboard RCA Audio, Kopfhörer, Subwoofer	DVI-D (HDCP), RGB (15-Pin), RGB/YUV (5x BNC), S-V, C-V	RGBHV, YUV, S-V, C-V S-V, C-V (RCA)	DVI, 2 × RGBHV (15-Pin, 5 × BNC), YUV (3 × RCA), YUV (BNC), S-V, C-V (BNC),	PC analog (15-Pin D-Sub), PC digital (DVI-D mit HDCP), YUV (BNC), S-V, C-V (BNC), Ausgang: PC digital (DVI-D, max. 4 Monitore im Loop)	PC analog (15-Pin D-Sub), PC digital (DVI-D mit HDCP), Ausgang: PC digital (DVI-D, max. 4 Monitore im Loop)
k. A.	RS232C	RS232C	RS232C	RS232C (9-Pin Sub-D) Ein-/Ausgang	RS232C (9-Pin Sub-D) Ein-/Ausgang
k. A.	optionale Videokarten	nein	nein	k. A.	k. A.
HDMI	ja	nein	k. A.	ja	k. A.
nein	nein	nein	nein	nein	nein
nein	nein	nein	nein	nein	nein
k. A.	1100 cd/m^2 o. Filterscheibe	600 cd/m^2	1300 cd/m^2 o. Filterscheibe	450 cd/m^2	450 cd/m^2
20 000:1	4000:1	1200:1	10 000:1	1800:1	2000:1
k. A.	340 W/0,5 W	480 W/1 W	420 W	325 W/3,5 W	550 W/2 W
k. A.	Colour Detail Adjustment	k. A.	k. A.	einstellbar	einstellbar
einstellbar	einstellbar	k. A.	k. A.	k. A.	k. A.
k. A.	k. A.	k. A.	k. A.	k. A.	k. A.
k. A.	k. A.	k. A.	k. A.	k. A.	k. A.
k. A.	k. A.	k. A.	k. A.	k. A.	k. A.
ja	ja	k. A.	k. A.	ja	ja
1232 × 722 × 120 mm	1222 × 736 × 99 mm	1348 × 800 × 130 mm ohne Fuß	1205 × 724 × 97 mm ohne Fuß	1254 × 742 × 149 mm ohne Fuß	1572 × 923 × 126 mm
38,3 kg	35,5 kg	48,3 kg	46,5 kg	44 kg	65 kg
k. A.	k. A.	Netz- und Signalkabel, Handbuch und Treiber auf CD, Fernbedienung inkl. Batterien, BNC auf Cinch-Adapter	Standard-Standfuß, Fernbedienung inkl. Batterien, Netz- und Signalkabel, Bedienungsanleitung	Netzkabel, Handbuch auf CD-ROM, Fernbedienung	Netzkabel, Handbuch auf CD-ROM, Fernbedienung
Bild-im-Bild	Bild-im-Bild, Videowall-Funktion	Bild-im-Bild	Bild-im-Bild	Bild-im-Bild, Split-Screen- Funktion, Lautsprecherausgang	Bild-im-Bild, Split-Screen- Funktion, Lautsprecherausgang; Sonderausführung PN-G655RE für Porträt-Dauerbetrieb

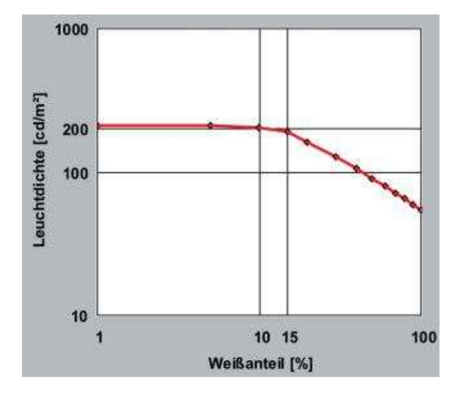
DLP steht für Digital Light Processing und bezeichnet ein überraschend einfaches, aber technisch anspruchsvolles bildgebendes Verfahren. Die Modulation der Lichtintensität wird hier nicht durch eine mehr oder weniger lichtdurchlässige Schicht erreicht, sondern durch das mechanische Verkippen winzig kleiner Spiegel. Das funktioniert im Prinzip wie ein kleiner Taschenspiegel, mit dem man Sonnenlicht auf eine weiße Hauswand ablenkt – wenn man den richtigen Anstellwinkel findet, entsteht ein heller Lichtpunkt an der gewünschten Stelle auf der Wand. Bei einem anderen Anstellwinkel eben nicht, genauer gesagt: woanders – dort, wo er nicht im Blickfeld liegt.

Der Lichtweg in einem DLP-Projektor ist so ausgelegt, dass das Licht vom Lampensystem auf den Spiegelchip fällt. Die Spiegelchen auf dem DLP-Chip, dem Digital Micromirror Device (DMD), lenken es im richtigen Winkel ins Projektionsobjektiv und erleuchten so die Leinwand.

Damit aus dieser Anordnung eine bildgebende Vorrichtung wird, braucht man allerdings viele Spiegel – genauso viele nämlich wie Bildpunkte – und sie müssen sehr klein sein, damit die gesamte Anordnung nicht so groß gerät wie ein Einfamilienhaus, sondern auf einen Chip von ein bis zwei Quadratzentimetern aktiver Fläche passt.

Spiegel im richtigen Winkel

Es lohnt sich, die erforderlichen Dimensionen zu berechnen, um ermessen zu können, wie erstaunlich es ist, dass dieses Verfahren funktioniert. Ein 0,55-Zoll-DMD in XGA-Auflösung hat beispielsweise eine aktive Fläche von circa 11,2 × 8,4 mm. Auf dieser Fläche gilt es, 1024 × 768, also insgesamt über eine dreiviertel Million Spiegelchen unterzubringen. Und nicht nur unterzubringen, sondern so zu lagern, dass sie sich mechanisch kippen lassen, um das Licht mal ins Projektionsobjektiv, mal auf einen Absorber zu lenken – je nachdem, ob das betreffende Pixel hell oder dunkel sein soll.



Mit entsprechenden Testbildern kann man die Leuchtdichte in Abhängigkeit vom Anteil weißer Bildflächen messen (Abb. 1).

Der Vorteil der DLP-Technik besteht darin, dass es innerhalb der konzipierten Lebensdauer des Projektors keine Komponenten gibt, die Alterungserscheinungen zeigen könnten. Abgesehen von der Lampe selbst als Verschleißteil. Daher eignen sich DLP-Projektoren besonders gut für den Dauerbetrieb, bei guter mechanischer und thermischer Auslegung sowie automatischem Lampenwechsel auch für den Einsatz über 24 Stunden pro Tag. Zwei weitere Vorteile haben DLP-Projektoren: Bei 1-Chip-Konstruktionen wird nur ein Lichtventil statt wie bei LCD drei eingesetzt – man spart zudem Strahlteiler und das Kreuzprisma für die Zusammenführung der Teilstrahlen. Dadurch kann man DLP-Projektoren vergleichsweise kompakt bauen, was für die Konstruktion von portablen Reiseprojektoren von Vorteil ist. Darüber hinaus lässt sich die Light Engine eines DLP-Projektors komplett kapseln, sodass er unempfindlich gegenüber Staub und Umwelteinflüssen wird – zumindest keine irreparablen Schäden an Nicht-Verschleißteilen davonträgt.

Regenbogen auf der Netzhaut

Ganz ohne Nachteile ist die DLP-Technik aber leider auch nicht. Diese betreffen vor allem die bei Weitem verbreitetsten 1-Chip-Projektoren. Die bekannteste potenzielle Problemzone ist der sogenannte „Regenbogeneffekt“. Das Gerät projiziert die drei RGB-Farbauszüge in schneller Folge nacheinander. Bewegt der Betrachter zufällig das Auge, landen die Farbauszüge eventuell nicht auf der gleichen Stelle der Netzhaut. Im ungünstigen Fall nimmt er sie als bunte Farbsäume (Regenbogen) in den drei Grundfarben wahr. Manche Hersteller versuchen, durch Verdopplung der Segmentzahl die Farbwechselfrequenz zu erhöhen und so den Effekt zu mindern.

Eine weitere Komplikation ergibt sich ebenfalls aus der Tatsache, dass die Projektion der drei Farbauszüge nacheinander erfolgt. Das Farbrad filtert jeweils nur eine der drei Grundfarben aus und verwirft den Rest. So gehen im Prinzip zwei Drittel der Lichtleistung verloren. Bei manchen Produkten versuchen die Hersteller, dies zu kompensieren, indem sie das Rad mit Filtern geringerer Farbsättigung bestücken. Diese lassen mehr Licht durch, allerdings um den Preis eines kleineren Farbraums. Zumindest früheren DLP-Projektoren wurde daher eine im Vergleich zu LCD schlechtere Farbwiedergabe nachgesagt.

Dem versucht man, mit verschiedenen Mitteln entgegenzuwirken. Ein Verfahren namens „Sequential Color Recapture“ verwendet ein spiralförmig mit Filterflächen belegtes Farbrad sowie einen vorgeschalteten Lichtintegrator und nutzt so unter dem Strich einen größeren Teil des Lichts. Die Ansteuerelektronik muss aber auf das anders strukturierte Farbrad angepasst sein.

„Brilliant Color“ arbeitet ebenfalls mit einer Modifikation des Farbrads und nutzt zusätzlich Filtersegmente in Mischfarben, etwa Cyan, Magenta und Gelb. Auch hier ist der Grundgedanke, möglichst viel Licht der Projektionslampe zu nutzen. Wird beispielsweise Gelb projiziert, braucht man Rot und Grün zusammen und müsste eigentlich nicht jeweils eine dieser Farben im Filterrad blocken. In diesem Fall kann man das gelbe Farbsegment zusätzlich nutzen und mehr effektive Lichtleistung für farbige Flächen erzielen.

Dies ist insbesondere bei DLP-Projektoren interessant, die die sogenannte Weißverstärkung nutzen, um Businessgrafiken mit farbigen Elementen auf weißem Grund heller projizieren zu können. Für diesen Zweck nutzen die Projektoren zusätzlich ein farbloses (weißes) Farbsegment, das allein dazu dient, weiße und schwach gesättigte Farben heller erscheinen zu lassen. Weiße Flächen sind dann also heller, als sie es durch die reine Kombination der Projektorgrundfarben Rot, Grün und Blau sein könnten, weil sozusagen zusätzlich weißes Licht am RGB-Farbmischprozess vorbeigeschleust wird.

Der Nachteil dieses Verfahrens ist, dass Weiß und schwach gesättigte Farben bei farbigen Medien wie Fotos oder Videos eventuell im Vergleich zu stark gesättigten Farben zu hell erscheinen, was im Prinzip einer Verformung der Gammakurven in den einzelnen Farbkanälen entspricht. Im Extremfall können dadurch in Farbverläufen wie bei blauem Himmel auf einem Foto sogenannte

Scheinkonturen, also Farbstufen, sichtbar werden. Aus diesem Grund fährt man die Weißverstärkung bei Videos normalerweise automatisch zurück. Generell ist es wünschenswert, das Ausmaß der Weißverstärkung einstellen zu können. Auf dem dieser Marktübersicht zugrunde liegenden Erfassungsbogen hat allerdings keiner der Hersteller Angaben zu diesem Punkt gemacht.

Zum Thema Lichtleistung sei für alle genannten Arbeitsprinzipien angemerkt, dass die Projektorlampen einer gewissen Fertigungsstreuung unterworfen sind und der gelieferte Lichtstrom bereits in den ersten 100 Betriebsstunden etwas sinkt. Daher sollte man bei der Berechnung der erforderlichen Lichtleistung eines Projektors einen Sicherheitszuschlag von 10 bis 15 Prozent einkalkulieren.

Grundsätzlich hat man bei Projektoren die Wahl zwischen Auf- und Rückprojektion. Erstere ist unkomplizierter – im Extremfall kann der Projektor einfach auf den Tisch stehen und auf eine weiße Wand projizieren. Eine Rückprojektion erfordert in der Regel eine Installation mit Einbau einer Rückprojektionsscheibe in dem betreffenden Raum, der wegen dieses zusätzlichen Platzbedarfs nicht zu klein sein darf. Ein Vorteil dieser Technik ist, dass sich keine Personen im Lichtweg befinden und Schatten auf die Leinwand werfen können.

Große Monitore ab einer Bilddiagonalen von circa 40 Zoll dienen nicht nur als Werbe- oder Info-Displays in Einkaufszentren, Flughäfen oder Bahnhöfen, sie haben auch ihren Platz in Konferenz- oder Seminarräumen. Ihr großer Vorteil liegt in einer relativ hohen Leuchtdichte und geringer Fremdlichtempfindlichkeit, weshalb sie besonders unter Tageslichtbedingungen gerne eingesetzt werden. Das ist für Konferenzen und Meetings nicht unwichtig, da sich die Teilnehmer in der Regel gern Notizen machen, und dafür ist eine ausreichende Beleuchtung wünschenswert.

Groß-Displays im mobilen Einsatz

Darüber hinaus lassen sich solche Groß-Displays wegen ihrer geringen Bautiefe gut an Wänden montieren oder in mobile Medienwagen integrieren – Letzteres ist besonders im Vermietbereich, etwa auf Messen oder in Konferenzhotels, interessant.

Da die Geräte in den vergangenen Jahren immer preiswerter geworden sind und gleichzeitig der Trend zu HDTV die native Auflösung hin zu Full-HD, also 1920 × 1280 Bildpunkten, getrieben hat, gibt es bei der Nutzung solcher Bildschirme als Computer-Display kaum noch Probleme. Moderne Grafikkarten können sowohl Full-HD bedienen als auch meistens Bewegtbilder in der gewünschten Qualität auf den Schirm bringen.

Welche Bilddiagonale man wählt, hängt im Allgemeinen von der Raumgröße ab – vom Budget sollte man sich zunächst möglichst nicht leiten lassen: Ein zu kleines Ausgabegerät birgt einen hohen Frustfaktor. Alle Anwesenden sollten auch die Beschriftung von Grafiken noch lesen können. Gängig sind derzeit Formate zwischen 40 und 65 Zoll – bei größeren Bilddiagonalen wird es schnell teuer, da bietet sich gegebenenfalls eine Rückprojektionslösung an.

Hinsichtlich der eingesetzten Technik hat der Kunde derzeit die Wahl

Projektoren

Hersteller	BenQ	Christie Digital Systems	LG Electronics	Liesegang	Mitsubishi	NEC Display Solutions
Website	www.benq.com	www.christiedigital.com	www.lge.com	www.liesegang.de	www.mitsubishielectric.de	www.nec-display-solutions.de
Produktname	MP723	LX 650	DX 535	dv 488active	XL650U/XL550	NP4000
Varianten	MP771 (Kurzdistanzobjektiv)	LX 450, LX 380	–	–	–	–
Preis (ohne MwSt.)	1764 €	auf Anfrage	1260 €	1428 €	3192 €/2688 €	4033 €
Marktbereich	Business-Präsentationen	Konferenzen, Präsentationen, Schulungsräume, kleinere Auditorien, kleinere Veranstaltungen	Business-Projektoren	Präsentationen	B2B	Konferenzen und Meetings
Bildgeometrie						
native Auflösung	1024 × 768 (XGA)	1024 × 768 (XGA)	1024 × 768 (XGA)	1024 × 768 (XGA)	1024 × 768	1024 × 768 (XGA)
max. Signalauflösung (interpoliert)	1080i	1600 × 1200 (VGA bis UXGA)	1440 × 1050 (SXGA+)	1280 × 1024 (SXGA)	PC: 1600 × 1200; Video: 1080i (1125i 50/60 Hz)	1600 × 1200 (UXGA)
Seitenverhältnis (nativ)	4:3	4:3	4:3	4:3	4:3	4:3
Funktionsprinzip	DLP	LCD	DLP	LCD	LCD	DLP
Anschlüsse						
Signaleingänge/-ausgänge	CV (Cinch), S-V, VGA, DVI (HDCP),VGA-out	DVI-D (HDCP), RGBHV (VGA), RGBHV/YUV (5 × BNC), C-V, S-V, YUV (3 × RCA), Monitor-out (analog)	VGA, DVI-I (HDCP), C-V, S-V, YUV	2 × VGA, Video (Chinch), S-V, RGB/YUV (15-Pin)	2 × VGA, DVI-D (HDCP), S-V, C-V RCA (L/R) für Video, Monitor: VGA (15-Pin) DC-out (5V), 1,5 A (max.)	RGBHV/YUV (15-Pin, 5 × BNC), DVI-I (HDCP), Mini-D-Sub, 15-Pin
Steuereingänge/-ausgänge	RS232, Mini-USB	RS232, USB (Typ B)	k. A.	RS232, USB	LAN, RS232C, USB	RS232C
modulare Eingangsbestückung	k. A.	k. A.	k. A.	nein	k. A.	k. A.
HDCP an DVI	ja	ja	ja	nein	ja	ja
WLAN für Steuerzwecke	nein	optional	nein	nein	ja	nein
WLAN für Datenübertragung	nein	optional	nein	nein	nein	nein
Leistungsdaten						
max. Lichtstrom	3300 ANSI-Lumen	k. A.	>95 %, 3500 ANSI-Lumen/ 2800 ANSI-Lumen	2800 ANSI-Lumen	4200 ANSI-Lumen/ 3100 ANSI Lumen	5200 ANSI-Lumen
Fullscreen-Kontrast	2000:1	2000:1	2000:1	500:1	600:1/400:1	k. A.
Leistungsaufnahme (Betrieb/Eco/Standby)	max. 365 W	5.0A bei 100 VAC, 4.1A bei 120 VAC, 2.1A bei 240 VAC; 480 W (max. 510 W)	270 W	250 W Standard	380 W/290 W	k. A.
Ausstattung						
motorische Objektiveinstellung	nein	ja	Autopositionierung, Tracking	nein	nein	ja
Wechselobjektiv	nein	0.8:1	k. A.	nein	k. A.	5 optionale Wechselobjektive mit Schnellverschluss
Zoombereich	1:1,10	1.3 – 1.8:1, 1.8 – 2.4:1, 2.4 – 4.3:1, 4.3 – 6.0:1	1,2 x/22,2 – 26,4	1,2-fach	1,48 – 1,78:1	motorisiert (1,0/1,34/1,32/ 2,0/1,87)
Farbmanagement	einstellbar	k. A.	16,7 Mio., 5-Segmente-Farbrad R/Y/G/W/B	einstellbar	Color Enhancer (Gamma Correction, RGB-TINT), Wall-Screen-Funktion (für beige, blaue, grüne, pinke und schwarze Wandfarben), 3D-Color-Uniformity-Korrektur	k. A.
Farbtemperatur	einstellbar	einstellbar	k. A.	einstellbar	k. A.	k. A.
Farbbalance	einstellbar	k. A.	k. A.	einstellbar	k. A.	k. A.
6-Achsen-Farbmanagement (RGB/CMY)	einstellbar	k. A.	k. A.	nein	k. A.	k. A.
Film-Modus (manuell/automatisch)	nein	k. A.	k. A.	manuell	k. A.	k. A.
HD-kompatibel	ja	alle HDTV/DTV-Formate bis 1080i	k. A.	nein	k. A.	k. A.
Sonstiges						
Lampenlebensdauer	Standard: 3000 Std.; Eco: 4000 Std.	1500 Std. bei max. Helligkeit; sonst: 2000 Std.	Standard: >2000 Std.; Eco: >2500 Std.	Eco: bis zu 3000 Std.; 36 Monate Herstellergarantie	Eco: ca. 5000 Std.	3 Jahre europaweiter Vor-Ort-Service; erweiterte Garantie für Daueranwendungen
Maße	275 × 129 × 310 mm	440 × 370 × 187 mm	346 × 263 × 109 mm	310 × 96 × 270 mm	333 × 113 × 272 mm	505 × 197 × 385 mm
Gewicht	3,5 kg	11,2 kg	4,4 kg	2,9 kg	4,7 kg/4,5 kg	16,5 kg
Lieferumfang	Quickstart Guide, Handbuch auf CD, Fernbedienung inkl. Batterien, Tasche, VGA- und Stromkabel	k. A.	Netz-, VGA-, S-Video- und Videokabel, Bedienungsanleitung, IR-Fernbedienung inkl. Batterien, Linsendeckel	Netz-, VGA, Video- und USB-Kabel, Schnellstartanleitung, CD-ROM mit Bedienungsanleitung und LightPen-Software, interaktiver Zeigestab, Fernbedienung	Kabelsatz, mehrspachige Bedienungsanleitung (CD-ROM) und Quickstart-Karte, Softbag, Fernbedienung inkl. Batterien	Netz- und Fernbedienungskabel; 6-Segment-Farbrad, Handbuch in 6 Sprachen, CD-ROM mit User Supportware, Objektiv-Schutzklappe, IR-Fernbedienung
Besonderheiten				Whiteboard-Funktion	optional: Deckenhalterung, WLAN-Adapter	2 austauschbare Farbräder (4-fach/6-fach) für unterschiedliche Anwendungen

Panasonic Deutschland	Samsung Electronics	Sanyo	Sharp Electronics (Europe)	Sony	Toshiba Europe
www.panasonic.de	www.samsung.de	www.sanyo.de	www.sharp.de	www.sony.de	www.toshiba.de
PT-D4000E	Crossover SP-A400B	PLC-XP100L	XG-F315X	VPL-CX155	ex20
–	–	schwarzes und weißes Gehäuse	–	–	ew25 (WXGA-Modell)
4117 €	1092 €	7800 €	1285 €	1932 €	1690 € (1990 €)
AV-Installation, Vermietung, Werbung, Präsentationen, E-Cinema (nur D-Serie)	POS, POI	Professional	Präsentationen, AV-Installationen	Präsentationen, AV-Installationen	Business, Education
1024 × 768 (XGA)	1024 × 768 (XGA)	1024 × 768 (XGA)	1024 × 768 (XGA)	1024 × 768 (XGA)	1024 × 768 (XGA)
1920 × 1080	1280 × 768 (WXGA)	1080i (UXGA)	1600 × 1200 (UXGA)	1400 × 1050 (SXGA)	RGB: 1600 × 1200 (UXGA), YpbPr: 1080p
4:3	15:9	4:3	4:3	4:3	4:3 (16:10)
DLP	DLP	LCD	DLP	LCD	DLP, Brilliant Color
RGBHV/YUV (5 × BNC), RGB (15-Pin) DVI-D (HDCP), C-V, (BNC), S-V,	HDMI, VGA, YUV, S-V, C-V	DVI-D (HDCP), 2 × RGBHV (VGA, 5 × BNC), 2 × YUV (BNC, Cinch), S-V, C-V, Monitorausgang: VGA	RGBHV, DVI-I, SV, YUV, CV	LAN, 2 × VGA, S-V, C-V	2 × RGBHV (15-Pin), S-V, C-V, YUV (via 15-Pin), RJ45, Monitorausgang: RGB
RS232C, 2 × Remote-in (Miniklinke, 9-Pin Sub-D parallel), LAN	RS232C	RS232, USB Typ B, KB-FB (3,5 mm Klinke)	RS232, LAN	RS232, LAN	LAN, RS232, USB Type A
nein	nein	Netzwerkintegration optional	k. A.	nein	nein
ja	HDMI	ja	ja	nein	nein
LAN (kabelgebunden)	nein	optional	LAN (kabelgebunden)	LAN (kabelgebunden)	RJ45
nein	nein	optional	nein	LAN (kabelgebunden)	RJ45
4000 ANSI-Lumen	2000 ANSI-Lumen	6500 ANSI-Lumen	3000 ANSI-Lumen	3500 ANSI-Lumen	2300 ANSI-Lumen (2600 ANSI-Lumen)
k. A.	2500:1	k. A.	2000:1	650:1	2000:1
520 W/15 W	260 W	490 W/392 W	349 W/11 W	285 W/7 W/0,5 W	350 W/290 W/9,5 W
vertikal: elektrisch/ horizontal: manuell	nein	ja	nein	nein	nein
ja	nein	nein	nein	nein	k. A.
1,3 – 8,4:1 mit Wechseloptiken (1,8 – 2,4:1 Standard)	k. A.	abhängig vom Objektiv	1:1,5	1:1,2	1:1,2
einstellbar	k. A.	k. A.	einstellbar	Farbbalance	k. A.
einstellbar	Standard: 6500 K; Modi: 5500 K, 6500 K, 8000 K, 9300 K	k. A.	einstellbar	niedrig, mittel, hoch	k. A.
einstellbar	k. A.	k. A.	einstellbar	ja	k. A.
einstellbar	k. A.	k. A.	einstellbar	k. A.	k. A.
manuell und automatisch	k. A.	k. A.	k. A.	k. A.	ja
ja	bis 1080i	nein	ja	bis 1080i	1080p
3 Jahre (Lampe: 6 Monate oder 500 Std.)	>3000 Std.	Standard: 2000 Std.; Eco: 3000 Std.	Standard: 2000 Std.; Eco: 3000 Std.	High: 2000 Std.; Standard: 3000 Std.	Standard: 2000 Std.; Eco: 3000 Std.
530 × 167 × 429 mm	343,1 × 162,4 × 347,2 mm	370 × 187 × 440 mm	315 × 109 × 280 mm	372 × 90 × 298 mm	337 × 118 × 265 mm
13,7 kg	4,5 kg	11,7 kg	4,1 kg	4,1 kg	4,2 kg
Netzkabel, Sicherungsseil, kabellose und kabelgebundene Fernbedienung	k. A.	Netz-, D-Sub15- und USB-Kabel, PIN-Code-Label, Lichtabweiser, Objektivadapter, IR-Fernbedienung mit Mausfunktion inkl. Batterien	Netzkabel, Bedienungsanleitung auf CD-ROM, RS232-Adapter, Tasche, Fernbedienung	Bedienungsanleitung auf CD-ROM, Kurzanleitung, RGB- und Netzkabel, Fernbedienung	Bedienungsanleitung auf CD-ROM, Schnellanleitung, RGB- und Stromkabel, Softcase, Fernbedienung inkl. Batterien und Laserpointer
			Auto-Keystone	Side-Shot (dig. Hor. Shift)	

zwischen Plasma und LCD, wobei die ganz großen Formate über 100 Zoll bisher noch der Plasmatechnik vorbehalten bleiben – zumindest was lieferbare Seriengeräte betrifft.

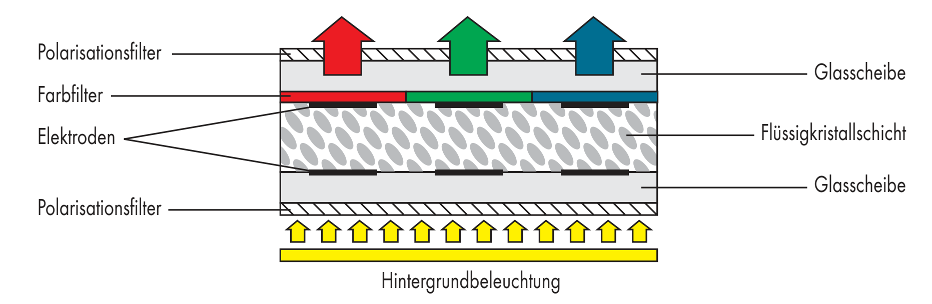
Früher erwies sich bei LC-Displays die Winkelabhängigkeit der Bildqualität, insbesondere des Kontrastes und der Farbwiedergabe, als Schwachpunkt. Der Grund dafür ist, dass Lichtstrahlen, die die Flüssigkristallschicht schräg durchlaufen und also von der Seite gesehen werden, einen längeren Weg in dieser Schicht zurücklegen, sodass deren Polarisationsebene stärker gedreht wird als bei Licht, das senkrecht durch das Panel hindurchtritt. Entsprechend dem veränderten Winkel ändern sich die Helligkeits- und Farbwerte, was in der Folge zu einer verfälschten Wiedergabe führen kann. Durch spezielle Maßnahmen im Panelaufbau und der Anordnung der Elektroden kann man diese Effekte heutzutage aber stark mildern, sodass sie nur noch bei extrem kritischen Anwendungen zu berücksichtigen sind.

Schwierig war es vor einigen Jahren auch noch, schnelle Bewegungen darzustellen. Der Schaltvorgang in einer LCD-Zelle erfordert eine mechanische Bewegung des Flüssigkristallmoleküls, die in einer Flüssigkeit naturgemäß nicht beliebig schnell vonstatten geht. Früher waren die Schaltzeiten so lang, dass bei bewegten Objekten im Bild Fahnen beziehungsweise Geisterbilder sichtbar waren. Durch entsprechende Ansteuerung der Displays sind die Schaltzeiten heutzutage allerdings so niedrig, dass etwaige Bewegungsunschärfen nur in kritischen Anwendungen wahrnehmbar sind.

Ein großer Vorteil der LCD-Technik ist, dass relativ hohe Leuchtdichten erzielbar sind. Professionelle Displays liefern Leuchtdichtewerte zwischen 350 und 450 cd/m^2 und sind daher tageslichttauglich – direktes Sonnenlicht auf dem Display vielleicht ausgenommen.

Offener Einblickwinkel bei Plasma

Ebenfalls tageslichttauglich und von Haus aus ohne Einschränkungen, was den Einblickwinkel angeht, sind Plasma-Displays. Mit dieser Technik wurden erstmals große Displays über 30“ Bilddiagonale wirtschaftlich herstellbar – heute teilen sich Plasma-Monitore den Markt mit LC-Groß-Displays.



Die Anordnung der Elektroden in einem LC-Display sorgt dafür, dass die Helligkeits- und Farbwerte nicht verfälscht werden, auch wenn die Lichtstrahlen die Flüssigkristallschicht schräg durchlaufen (Abb. 2).

Technisch arbeitet ein Plasma-Display ähnlich wie eine Leuchtstoffröhre, allerdings funktioniert die Anregung etwas anders. Die Plasmaentladung erfolgt nicht kontinuierlich, sondern als Folge kurzer Einzelentladungen (Burst). Je länger ein solcher Burst ist, desto heller erscheint das betreffende Pixel, weil das Auge die Helligkeit der Einzelentladungen über die Bildwiederholperiode zusammenfasst. Der eigentliche Fluoreszenzprozess geht sehr schnell vonstatten, deshalb können die Einzelentladungen extrem kurz sein und relativ viele Entladungen aufeinanderfolgen. Ein Plasma-Display kann somit von Haus aus die effektive Helligkeit eines Pixels feinfühlig steuern. Die erreichbaren Kontrastwerte sind – zumindest in verdunkelten Räumen – ebenfalls hoch. Ein Fullscreen-Kontrast von 2500:1 und mehr ist durchaus erreichbar, während die Kontrastwerte bei LC-Displays meist unter 1000:1 bleiben.

Moderne Plasma-Displays liefern gemessene Leuchtdichten meist im Bereich zwischen 150 und 250 cd/m^2. Dabei ist allerdings zu berücksichtigen, dass die maximale Leuchtdichte durch den Bildinhalt bedingt ist. Das hängt damit zusammen, dass nicht wie bei LCDs eine konstant leuchtende Lichtquelle, sondern die Summe der einzelnen Plasmaentladungen das Licht erzeugt. Diese Summe darf aber nicht beliebig groß werden, da sonst eine Überlastung des Displays und der Stromversorgung zu befürchten wäre. Eine Schutzschaltung begrenzt daher die maximale Gesamtleistung. Einen ähnlichen Effekt gibt es bei Röhrenmonitoren, bei denen eine Strahlstrombegrenzung die maximale Helligkeit limitiert.

Eine gleichmäßig weiße Bildfläche hat aber zwangsläufig eine niedrigere Helligkeit als ein kleiner weißer Punkt in einem ansonsten schwarzen Bildschirm. In der Tat kann man mit speziellen Testbildern die Leuchtdichte in Abhängigkeit vom Anteil weißer Bildflächen messen und etwa das in Abbildung 2 gezeigte Ergebnis erhalten. In der Praxis kommen die mit einem Weißanteil von 15 % gemessenen Leuchtdichtewerte dem visuellen Eindruck im Vergleich mit anderen Bildschirmtypen schon recht nahe. Sofern man nicht hauptsächlich mit großen, weißen Flächen, etwa als Hintergrund für Grafiken, zu tun hat, sollte das ausreichen. Wer eine höhere Leuchtdichte benötigt, sollte vorab den visuellen Eindruck anhand repräsentativer, eigener Musterbilder überprüfen.

Ebenfalls aus früheren Zeiten bekannt ist der sogenannte Einbrenneffekt. Lässt man Standbilder längere Zeit unverändert auf einem Plasma-Display stehen, bleiben sie eine Zeit lang als eine Art schattenhaftes Geisterbild sichtbar, selbst wenn der Bildinhalt sich inzwischen geändert hat. Im Prinzip resultiert dieser Effekt daraus, dass die Plasmaentladung in unmittelbarer Nähe der Leuchtstoffschicht stattfindet und diese im Laufe der Zeit verändert. Wenn die Leuchtstoffe einer länger dauernden Entladung ausgesetzt waren (beispielsweise einem längeren Burst), leuchten sie nicht mehr ganz so hell wie zuvor. Die betreffenden Zellen sind auch dann noch etwas dunkler, wenn sich die Bildinhalte verändert haben.

Weil dies ein wichtiger Punkt ist, haben die Hersteller an dieser Stelle besonders intensiv geforscht und zum einen Leuchtstoffe entwickelt, die nicht mehr so einbrennempfindlich sind, und zum anderen Hilfsmittel in ihre Displays eingebaut, die die sichtbaren Effekte des Einbrennens mildern sollen. So gibt es zum Beispiel seit Langem spezielle, eingebaute Refresh-Programme, die durch Wiedergabe von Weißflächen oder invertierten Bildern eine möglichst gleichmäßige Belastung aller Zellen sicherstellen sollen. Auf diese Weise ergibt sich mit der Zeit lediglich eine geringfügige

Senkung der Gesamthelligkeit ohne die ausgeprägten Geisterbilder. Ganz verschwunden ist der Effekt allerdings trotz allem nicht, sodass Anwender, die von vornherein wissen, dass ihre Displays mit Standbildern beaufschlagt werden (Flughafen, Bahnhof), Alternativen zumindest in Erwägung ziehen sollten.

Hohe Kontrastwerte sind – bei Projektoren ebenso wie bei Groß-Displays – nur dann interessant, wenn der Raum vollständig abgedunkelt werden kann, sodass Fremdlicht keinen Einfluss nimmt. In Räumen mit Fremdlichteinfluss – beispielsweise einer Restbeleuchtung für Mitschriften – erzeugt dieses Licht durch diffuse Reflexion an der Oberfläche des Displays beziehungsweise der Projektionsleinwand bereits eine gewisse Helligkeit, die den maximalen Kontrastumfang mitunter deutlich begrenzt. Wer auf kontrastreiche Bilder in Umgebungen mit Fremdlichteinfluss, respektive künstlicher Beleuchtung, Wert legt, ist oft besser beraten, sich um die Lichtführung in der Umgebung des Displays zu kümmern, als ein Gerät mit einem besonders hohen Kontrastwert zu kaufen. Insbesondere sollte eine direkte Beleuchtung des Bildschirms respektive der Leinwand möglichst vermieden werden. Wenn dies nur eingeschränkt machbar ist, muss das Display beziehungsweise der Projektor eine ausreichende Helligkeit liefern können, um den gewünschten Bildkontrast aufrechtzuerhalten.

Signalverwaltung sorgt für Komfort

Viele Projektoren und Displays verfügen von Haus aus über mehrere Eingänge für PCs und Videoquellen, sodass man beim Wechsel der Zuspielquelle nicht unbedingt das Anschlusskabel umstecken muss. Oft gibt es entsprechend viele Audioeingänge oder doch je einen für PC- und Videoquellen, die mit der Eingangswahl passend umgeschaltet werden (Audio follows Video).

Diese eingebaute Signalverwaltung sollte man sich nach Möglichkeit zunutze machen, denn sie erlaubt einen reibungslosen Wechsel beispielsweise zwischen zwei Vortragenden mit eigenem Notebook ohne lästige und unprofessionell wirkende Unterbrechungen durch Kabelumstecken. Manche Geräte haben auch eine Bild-im-Bild-Funktion, die es erlaubt, Videos in gewünschter Größe und Position in die PC-Präsentationsgrafik einzublenden. Noch komfortabler sind sogenannte Presentation Switcher, die die Signalumschaltung extern erledigen und deren Bedienelemente man zum Beispiel ohne Schwierigkeiten in ein Rednerpult einbauen kann. Hier begibt man sich allerdings bereits in den weiten Bereich der installierten Mediensysteme, die ganz auf die jeweilige Anwendung zugeschnitten werden können. Eine reibungslose Standardpräsentation ist oft aber schon mit Bordmitteln realisierbar. Bei einer Installation im Firmenumfeld mit Netzwerkzugang kann eventuell eine LAN-Schnittstelle – oder ein Projektor mit WLAN-Fähigkeit – dazu dienen, das Präsentationsgerät über das Netz zu steuern oder sogar Daten zu ihm zu übertragen.

Datenprojektoren und Displays sind üblicherweise für die Wiedergabe von Präsentationen ausgelegt. Sie bieten aber in der Regel die Möglichkeit, Videozuspielungen in guter Qualität wiederzugeben, oft sogar mit speziellen Betriebsarten für die Wiedergabe zum Beispiel von Kinofilmen auf DVD (Film-Modus). Das funktioniert normalerweise ganz gut, allerdings ist das Umrechnen der bei Video (NTSC und PAL) üblichen Sequenz von Halbbildern in eine von Vollbildern anderer Auflösung – nämlich derjenigen des DLP- respektive LC-Panels – keine triviale Angelegenheit. Es gibt dabei verschiedene Hürden, von denen einige damit zusammenhängen, dass sich im Video dargestellte Objekte zwischen zwei Halbbildern bewegen, zwei solcher Halbbilder nun aber zu einem zusammengerechnet werden müssen, um die notwendige Progressive-Scan-Ansteuerung des Display-Panels zu ermöglichen. Wenn das schiefgeht, sieht man an bewegten Kanten im Bild Treppchen („jaggies“) oder gar ausgefranste Kanten („feathering“). Allerdings: Will man dieses keineswegs kleine Problem in sehr guter Qualität lösen, ist der Aufwand schon recht hoch, sodass nicht jedes Produkt seinen Schwerpunkt in diesem Bereich hat.

Wer kopier- oder abspielgeschützte Inhalte (etwa Kinofilme) über digitale Verbindungen dem Wiedergabegerät zuspielen will, sollte darauf achten, dass das Gerät entweder einen HDMI-Eingang hat oder zumindest am DVI-Eingang das HDCP-Protokoll anbietet.

Die in den Tabellen aufgeführten Daten basieren auf Angaben der Hersteller, die sich zum Teil technische Änderungen vorbehalten. Einen Anspruch auf Vollständigkeit erhebt die Übersicht nicht.

Die meisten Hersteller haben bei Projektoren und Groß-Displays für den professionellen Einsatz mehrere Modelle in verschiedenen Leistungsstufen beziehungsweise Bildformaten im Programm, um dem Anwender die Möglichkeit zu geben, das Präsentationsgerät genau auf die jeweilige Anwendungssituation anpassen zu können. Der für den vorliegenden Beitrag verfügbare Platz reicht leider nicht aus, um alle Produktvarianten aufführen zu können.

Beschränkungen der Übersichtstabelle

In vielen Fällen unterscheiden sich die Produkte einer Geräteklasse – so zum Beispiel bei den Groß-Displays – jedoch nur hinsichtlich der Bildschirmgröße bei ansonsten vergleichbarer oder ähnlicher technischer Ausstattung. Bei Projektoren für mittlere bis große Konferenzräume und ähnliche Anwendungen gibt es ebenfalls bei den meisten Herstellern ein Mittelfeld in einem Bereich von 3000 bis 5000 ANSI-Lumen, in dem sich die kleineren von den größeren Systemen zwar durch Ausstattungsdetails wie Motor-Zoom und Lens-Shift unterscheiden, ansonsten aber recht ähnlich sind.

Wir haben daher pro Hersteller einen Projektor aus dieser Mittelklasse gewählt, wobei wegen der etwas unterschiedlichen Strukturierung der Schwerpunkte innerhalb der Produktlinien in den zurückgesandten Erfassungsbögen nicht immer hundertprozentig korrespondierende Geräte gefunden werden konnten.

Bei den Groß-Displays sind wir ähnlich vorgegangen und haben uns auf den Bereich 50 bis 65 Zoll konzentriert, der besonders für den Vermietbereich und als Projektorersatz in Besprechungsräumen interessant ist. 40- bis 42-Zoll-Displays hat eigentlich fast jeder Hersteller in verschiedenen Auflösungen schon seit Längerem im Programm, weil dies die Brot-und-Butter-Info-Displays sind. Sie tauchen in der Tabelle jedoch nicht auf, weil sie ähnlich ausgestattet sind wie die größeren Systeme und durch ihre Anzahl das verfügbare Format sprengen würden. (ka)

DIETER MICHEL

arbeitet als freier DV-Journalist und ist Chefredakteur der Fachzeitschrift Prosound.



AIX 6.1 mit neuen Sicherheitsfunktionen

Allmachtsende

Andreas Leibl

IBMs hauseigenes Unix hat den Ruf, besonders sicher zu sein, da es in Banken und Großunternehmen verbreitet ist. Mit der neuen Version 6 haben die Entwickler eine ganze Reihe neuer Schutzmechanismen hinzugefügt.

Das Thema Sicherheit bewegt die IT-Branche wie wenig andere. Nachdem sich herumgesprochen hat, dass Systeme nicht sicher sind, bloß weil sie proprietär oder weniger verbreitet als das Heim-PC-Windows sind, bemühen sich alle großen Unix-Hersteller um Verbesserungen. Staatliche Vorschriften vor allem für Unternehmen sorgen für zusätzlichen Auftrieb auf dem Sicherheitsmarkt.

Neue Versionen von Betriebssystemen wie AIX 6.1 bieten in mehreren Bereichen neue Funktionen oder werten ältere auf. IBMs Unix bringt von Haus aus zwei Filesysteme mit: das „alte“ JFS (Journaled File System) und das neuere JFS2 (Enhanced JFS). Es hat inzwischen einige Release-Wechsel hinter sich und gilt als stabil. Weiterentwicklungen gibt es nur noch bei JFS2. Das Verkleinern von Filesystemen – seit AIX 5.3 verfügbar – funktioniert nur mit JFS2, nicht mit seinem Vorgänger. Den Wegfall von Kompression auf Filesystem-Ebene, die das alte JFS noch beherrscht, kann man getrost verschmerzen.

Mit AIX 6.1 lernt JFS2, Daten zu verschlüsseln. Im Gegensatz zu anderen Produkten geschieht das auf Dateiebene und nicht für das gesamte Block Device. Das hat den Vorteil, dass man die verschlüsselten Dateien ganz normal sichern kann und sie auf dem Backup-Medium nicht im Klartext auftauchen. Mit dem berühmten Band, das beim Transport vom Laster fällt, weiß der unehrliche Finder nichts anzufangen.

Dateiweise Verschlüsselung

Jede Datei besitzt ihren eigenen Schlüssel, der in den erweiterten Dateiattributen hinterlegt ist. Zum Schutz nutzt JSF2 den Schlüssel des Benutzers, der wiederum passwortgesichert abgelegt ist. Soll die Datei für eine Gruppe les- oder schreibbar sein, können die Mitglieder über den sogenannten Keystore der Gruppe an die Datei herankommen.

Beim Entschlüsseln geht der Kernel blockweise vor, so wie er sie von der Platte liest. Wer also eine 2 GByte große Datei öffnet, aber nur einen Block daraus liest, muss nicht auf die Entschlüsselung der ganzen Datei warten. Einmal entschlüsselte Blöcke liegen wie andere im Filesystem-Cache und müssen bei einem wiederholten Lesevorgang nicht jedes Mal durch den Entschlüsselungsalgorithmus.

In des Kernels Tiefen

Das Ganze klingt kompliziert, läuft für den Benutzer aber weitgehend transparent ab. Sobald sein Keystore geöffnet hat (beim Login oder später), lädt das System die Schlüssel in den Kernel und alle weiteren Dateioperationen laufen transparent ab. Lediglich ein kleines Flag „e“ für „encrypted“ in der Ausgabe von *ls* weist auf die Verschlüsselung hin.

```
ls -U geheime_daten.txt
-rw---e   1 bob users    12345 Sep 18 06:00
geheime_daten.txt
```

Ohne das Passwort für den Keystore ist kein Zugriff auf die entschlüsselte Version der Datei möglich. Das gilt selbst für Root. Er müsste dem Benutzer schon einen Trojaner unterschieben, wollte er an das Passwort heran, um damit den Keystore zu öffnen. Standardmäßig, im Root Admin Mode kann er das Passwort für den Benutzer-Keystore zwar zurücksetzen, befindet sich der „Schlüsselkasten“ aber im Root Guard Mode, ist ihm das verwehrt. Damit die Keys nicht auf Umwegen im Klartext erscheinen, hat

IBM den Kernel Dump modifiziert, sodass Access Keys in einem Dump nicht auftauchen.

Als Verschlüsselungsmethode stehen standardmäßig zur Wahl: 128 Bit AES CBC, 192 Bit und 256 Bit CBC und ECB. Die Benutzerschlüssel zum Schutz der Filekeys sind per Default 1024 Bit lange RSA Keys, bei Bedarf kann man 2048 oder 4096 Bit lange Schlüssel verwenden.

Wer eine Dateiverschlüsselung will, muss sie explizit einschalten. Für Workload Partitions (WPAR) – vergleichbar mit einer BSD Sandbox oder Suns Containern – muss das auf der primären Partition geschehen, danach steht sie auf allen WPARs zur Verfügung. Damit nicht jeder Ramsch durch die Krypto-Routinen geht und damit unnötiger Overhead entsteht, gehen sie dateiweise vor. Zur Vereinfachung kann der Zuständige ein Verzeichnis oder Filesystem markieren, sodass alle darin neu angelegten Dateien die Verschlüsselungseinstellung erben; bereits vorhandene bleiben unberührt.

Zur Steuerung der kryptografischen Fähigkeiten des Encrypted File Systems genügen drei Kommandos:
– *efsenable* aktiviert das Encrypted File System,
– *efskeymgr* verwaltet Keystores und den Zugriff darauf und
– *efsmgr* dient der Ver- und Entschlüsselung von Dateien und verwaltet sie.

Das Ende der Allmacht

Der Overhead beim Platzverbrauch soll nach IBM-Angaben vernachlässigbar sein: Eine Datei, die unverschlüsselt 2 KByte groß ist, soll auch verschlüsselt etwa 2 KByte groß bleiben. Zur Lese- und Schreibperformance gibt es noch keine offiziellen Angaben. Da in der Open-Beta-Ausgabe von AIX 6 leider die erforderlichen kryptografischen Bibliotheken fehlten, war eine Performancemessung nicht durchführbar.

Das traditionelle Unix-Sicherheitskonzept mit Benutzern und Gruppen sowie einem Superuser *root*, der alles darf, ist in die Jahre gekommen und zeigt gefährliche Schwächen. Vor allem, wenn man Evidenzen für ein Audit vorlegen muss, steigt der Aufwand für Sicherung und Logging erheblich. Deshalb hat IBM in AIX 4.2.1 bereits ein wenig beachtetes Rollensystem (Role Based Access Control, kurz RBAC) eingeführt, das aber Änderungen im Programmcode erforderte und wohl deshalb kaum jemand benutzt hat. Es steht weiter als „Legacy RBAC“ zur Verfügung. Mit Version 6 erscheint das neue „Enhanced RBAC“, das ohne Anpassungen der Software auskommt und darüber hinaus nicht nur den Zugriff auf Programme, sondern auch auf Dateien und Devices regeln kann.

Bei einer Standardinstallation ist Enhanced RBAC eingeschaltet. Die vordefinierten Policies sind so gestaltet, dass sich das System nicht anders verhält als ein AIX ohne RBAC. Ausschalten lässt es sich, indem man auf das alte System zurückschaltet, was man sich aber genau überlegen sollte, weil andere Features wie WPAR und EFS das neue RBAC zwingend brauchen.

Intern arbeitet RBAC mit sogenannten „Authorizations“, die einen Schlüssel zu Kommandos oder anderen Funktionen darstellen. Schlüssel sind zu Rollen zusammengefasst, die wiederum Benutzern zugewiesen sind. Die Rollen funktionieren wie ein Schlüsselbund und können aus einer Mischung von Schlüsseln mit anderen Rollen bestehen. Jede Authorization kann in mehreren Roles vorkommen, jeder Benutzer eine oder mehrere Rollen haben.

Will man den Zugriff auf ein Programm mittels RBAC regeln, legt man zunächst eine Authorization für das Programm an, weist die einer Rolle zu und teilt sie schließlich einem oder mehreren Benutzern zu. Im Gegensatz zu Security Enhanced Linux (SELinux) ist RBAC „authoritative“: Selbst wenn die Dateiberechtigungen das Lesen/Schreiben/Ausführen verbieten, kann man den Zugriff per RBAC dennoch gewähren.

Authorizations haben bis zu 63 Zeichen lange Namen und bilden einen hierarchischen Namensraum. Alle vom Betriebssystem vordefinierten beginnen mit *aix.*, etwa *aix.system.abc*. Der Administrator kann sie nicht ändern. Wer *aix.system* an seinem Schlüsselbund hat, bekommt automatisch alle nachgeordneten Authorizations mit. Kunden können sich in eigenen Namensräumen mit bis zu neun Stufen austoben, wie bei *de.heise.ix.redaktion.assistenz.automaten.heiss getraenke*. Ähnliche Regeln gelten für die Rollen. Im Gegensatz zu den Authorizations kann der Admin aber vordefinierte AIX-Rollen modifizieren.

Drei RBAC-Rollen stellen exemplarisch die verbreitetsten Tätigkeitsprofile nach:
– Information Systems Security Officer (ISSO): Er verwaltet die Sicherheitsrichtlinien und ernennt SAs und SOs,
– System Administrator (SA): Er hat weitreichende Befugnisse, kann aber im Gegensatz zum ISSO nicht die Sicherheitsrichtlinien ändern und sich mehr Macht verschaffen und
– System Operator (SO): Er ist für normale Systemverwaltungsarbeiten und Fehleranalyse zuständig.

Rollen sind, anders als die Zugehörigkeit zu AIX-Gruppen, nicht automatisch nach dem Login wirksam. Der Benutzer muss eine oder mehrere seiner Rollen explizit mit dem Kommando *swrole* aktivieren und dafür noch einmal sein Passwort eingeben. Damit will IBM verhindern, dass ein unbewachtes Terminal böswilligen Findern gleich alle Rechte des unvorsichtigen Benutzers verschafft. Jeder Rollenwechsel erzeugt eine neue Shell, mit deren Beendigung der Benutzer wieder auf seinen vorherigen Stand an aktivierten Berechtigungen zurückfällt. Seine aktivierten Rollen kann der Benutzer mit dem *id*-Kommando abfragen, das in AIX 6 neben der User-ID (uid) und Gruppen-ID (gid) auch die gerade aktiven Role-ID(s) (rid) ausgibt. Ist ein Eintippen des Passworts nicht möglich, etwa weil ein per Cron gestarteter Job das verhindert, kann der Administrator für den entsprechenden User Default Roles eintragen, die automatisch aktiv sind.

Regelt RBAC den Zugriff auf Dateien, darf der Anwender darauf nur nach Aktivierung einer passenden Rolle und mit einem modifizierten *vi* namens *pvi* (privileged *vi*) zugreifen. Ob in Zukunft weitere Editoren hinzukommen werden, war nicht in Erfahrung zu bringen. Da der Streit über den „richtigen“ Editor in etwa so alt ist wie Unix

iX-TRACT

- Mit der neuen Version AIX 6.1 hat IBM grundsätzliche Veränderungen am Sicherheitskonzept durchgeführt.
- Damit haben die Entwickler die in die Jahre gekommenen Zugriffsrechte von Unix modernisiert und erweitert.
- Die Maßnahmen haben in einem Fall zu einer Portierung des File Permission Manager auf die Vorversion 5.2 geführt.

selber, dürfte für heftige Diskussionen gesorgt sein.

Sind mehrere Systeme auf diese Weise zu verwalten, kann der Administrator die RBAC-Datenbanken auf einen LDAP-Server stellen und zentral verwalten. Hat man Geschmack an der neuen Rechteverteilung gefunden, fehlt nur noch der letzte, große Schritt, um den magischen Superuser *root* mit der ID 0 zu entmachten. Durch *root user disablement* kann sich nicht nur keiner mehr als *root* an der Maschine anmelden oder auf den User wechseln, sondern die ID 0 verliert auch ihre privilegierte Rolle im System: Alle Checks nach dem Muster „aber wenn die ID gleich null ist, darf er doch“ schlagen fehl. Damit gewinnt man ein erhebliches Maß an Sicherheit, denn alle Exploits, die zum Beispiel über einen Buffer Overflow Root-Rechte erschleichen, sind damit harmlos. Dennoch sollte man den Schritt erst nach ausgiebigen Tests in Erwägung ziehen, da man sonst das System nicht mehr nutzen kann, wenn man etwas übersehen hat.

Trau, schau, wem!

Zu kontrollieren, wer welches Programm ausführen kann, ist aber nur die halbe Miete. Wenn eins startet, will man sicher sein, dass das Kommando nicht in irgendeiner unerwünschten Weise verändert wurde, sei es, weil jemand die Datei modifiziert oder weil er ein gleichnamiges Programm geschickt im Suchpfad platziert hat, was besonders leicht gelingt, wenn das aktuelle Verzeichnis (der einsame Punkt „.“) im Suchpfad steht.

Das lässt sich verhindern, wenn eine vertrauenswürdige Datenbank mitteilt, wo das Programm zu stehen hat, und an einer Hash-Summe ungewollte Veränderungen erkennt. Modifizierte oder falsch platzierte Programme und Bibliotheken lädt das System gar nicht erst, geschweige denn, dass es sie ausführt. Bei AIX 6 heißt das „Trusted Execution“.

Prüfungen sind sowohl statisch, durch den Systemadministrator auf Anfrage, regelmäßig oder grundsätzlich bei jedem Aufruf durchführbar. Sicherheit und Performance sind sich widersprechende Ziele: Je mehr Checks stattfinden und je sicherer die Prüfsummen sind, desto höher der Preis, den man bei der Geschwindigkeit des Systems zahlt. Deshalb lässt sich der Check in Stufen zu- und abschalten: die Hash-Summen für Programme und Bibliotheken kann das System in SHA-1, SHA-256 und SHA-512 berechnen, und es kann die Werte noch einmal signieren. Was von den AIX-Installations-CDs kommt, hat IBM mit Hash-Code versehen und signiert. Ein Verifizieren der Signaturen findet nur auf Wunsch und bei der statischen Überprüfung des Systems statt, jedoch nicht beim Laden beziehungsweise Ausführen von Code. Es gibt zwei Modi:

– Statisch: Das Tool „System Integrity Check“ dient zur Überprüfung der Integrität des installierten Systems, vergleicht die Prüfsummen von Programmen mit denen der Signaturdatenbank und gegebenenfalls den Zertifikaten für die signierten Hashes.
– Runtime: Hier findet ein Vergleich der Prüfsummen der zu ladenden Programme und Bibliotheken mit der Hash-Datenbank statt, Signaturen bleiben aus Performancegründen unberücksichtigt.

Alle Prüfungen und Policies kann der Zuständige jederzeit an- und ausschalten, wobei die Aktivierung sofort, die Deaktivierung erst nach einem Reboot wirksam wird, was möglichen Einbrechern das Leben erschweren soll. Prüfungen lassen sich auf Teilbereiche einschränken. Für maximale Sicherheit kann man sogar Root verbieten, die entsprechende Datenbank zu modifizieren, indem man die Signaturdatenbank sperrt.

Trusted Execution (TE) ist inkompatibel zu einem älteren AIX-Feature namens Trusted Computing Base (TCB). Das musste bereits bei der Installation aktiviert werden. Ist das geschehen, verweigert TE seine Dienste. TE lässt sich anderenfalls nach dem Installieren noch aktivieren. Darüber hinaus bietet TCB nicht nur schlechtere, weil nicht kryptografisch sichere Prüfsummen, sondern muss auch bei der Laufzeitprüfung passen. Lediglich periodische Integritätschecks sind wie bei TE durchführbar.

Sicherheit auf Expertenebene

Eigentlich nicht neu ist der AIXPert, ein Werkzeug zur einfachen Verwaltung von Sicherheitseinstellungen in AIX. Zuerst kam es vor einem Jahr als Teil des Technology Levels 5 (TL 5) von AIX 5.3 heraus. In AIX 6 haben es die Entwickler aber erweitert und aufgewertet, indem sie es vom Expansion Pack in das AIX-Basispaket verschoben haben.

AIXPert installiert keine neuen Features, sondern ändert lediglich Einstellungen des Standards von AIX, das aber in erheblichem Umfang. Selbst in der niedrigsten Sicherheitsstufe führt es Hunderte Änderungen durch.

Vorkonfiguriert sind drei Level: niedrig, mittel und hoch. Der Administrator kann aber jede einzelne Einstellung ändern beziehungsweise Punkte aktivieren und deaktivieren, um die Stufe den eigenen Bedürfnissen anzupassen. Sie orientieren sich an den Empfehlungen US-amerikanischer Behörden und Standardisierungsgremien wie dem National Institute of Standards and Technology (NIST).

AIXPert arbeitet intern mit einer XML-Datenbank, in der alle Regeln und Einstellungen abgelegt sind. Dadurch ist es flexibel und erweiterbar, ab AIX 6 dürfen Kunden eigene Regeln für AIXPert nach dem offengelegten XML-Schema entwickeln. Für die meisten Einstellungen generiert AIXpert automatisch Undo-Operationen und speichert sie, sodass man schnell und einfach auf einen älteren Stand der Einstellungen zurückgehen kann. Durchgeführte speichert es in einem XML-File namens *appliedaixpert.xml*, das man auf andere Systeme verteilen kann, um dort die identischen Einstellungen nachzuziehen, was bei einer großen Anzahl verwalteter Systeme zu erheblicher Zeitersparnis führt. Dieselbe Datei kann zur Überprüfung der Systemeinstellungen (etwa per Cron-Job) dienen, ungewollte Änderungen fallen dadurch schneller auf. Bei Systemen, die der Administrator über das Netz installiert (NIM), kann AIXPert als Postinstall-Action laufen und das

Sicherheit in AIX 6.1

Encrypted File System (EFS): Im Kernel eingebundenes Verfahren zur blockweisen Ver- und Entschlüsselung von Daten.

Role Bases Access Control (RBAC): Erlaubt das differenzierte Zuweisen von Rechten selbst für den Superuser.

Trusted Execution (TE): Über Prüfsummen und genaue Kontrolle der Lage im Dateisystem schützt AIX 6 das System vor Schadsoftware.

AIX Security Expert (AIXPert): Werkzeug zur Verwaltung der Sicherheitseinstellungen im Betriebssystem.

File Permission Manager (FPM): Ursprünglicher Bestandteil von AIXPert, zurückportiert auf AIX 5.2 zum Ändern der dortigen Dateiberechtigungen.

System sofort nach dem Installieren absichern. Neu ist die Möglichkeit, Templates von einem LDAP-Server zu holen und geänderte Sicherheitseinstellungen einfacher zu verteilen.

Während die Entwickler von AIXpert bei der Sicherheitsstufe „niedrig“ vor allem Wert darauf gelegt haben, möglichst wenig zu behindern und nur nicht-invasive Maßnahmen ergriffen haben, schaltet die mittlere Stufe bereits einen Schutz gegen Portscans ein. Unsichere Remote-Zugänge bleiben aber noch erlaubt, wie *telnet*, *ftp* und *r*-Kommandos. Erst die Sicherheitsstufe „hoch“ dekonfiguriert die Dienste und aktiviert eine Firewall, die alle Ports blockiert, die zum Zeitpunkt der Konfiguration unbenutzt sind, das heißt auf denen gerade kein Dienst lauscht. Will man später neue Dienste anbieten, muss man die Firewall explizit anpassen.

Zusätzlich zu den Sicherheitsstufen gibt es noch einen „SOX Compliance Assistent“. Mit nur vier Schaltern lassen sich Empfehlungen von SOX-COBIT (www.sox-online.com) in Gruppen auf dem System umsetzen.

Eine GUI ermöglicht es dem Auditor, die Einhaltung der Regeln auf dem System zu überwachen. Der File Permission Manager (*fpm*) war ursprünglich ein Teil von AIXPert. Die Entwickler haben ihn auf AIX 5.2 zurückportiert. Er ändert die Berechtigungen der Dateien in der AIX-Standardinstallation und bietet wie der AIXPert drei Sicherheitsstufen. Je nach Stufe entfernt *fpm* zwischen 233 und 278 Bits der Set User ID (*suid*), nur etwa 60 bis 100 bleiben unangetastet. Mit anderen Worten: drei Viertel der Bits, wie sie eine Standardinstallation setzt, sind überflüssig oder sogar gefährlich. Wie AIXPert legt *fpm* vor den Änderungen einen Snapshot der aktuellen Konfiguration an, sodass eine Rückkehr einfach vonstatten geht.

Fazit

IBM hat bei der neuen Versions AIX 6.1 das Schwergewicht auf die Sicherheit gelegt und damit das Ende der klassischen Zugriffsberechtigungen in Unix eingeläutet. Zu den besonderen Features gehören das blockweise Verschlüsseln von Daten im EFS, das Lagern der Schlüssel im Keystore, sodass auch Gruppen gemeinsame Schlüssel nutzen können und die rollenbasierte Zugangskontrolle, die dem Root seiner bisherige Machtfülle nimmt.

Trusted Execution, die das Laden von unwillentlich modifizierten Programmen und Bibliotheken verhindert, sowie AIXPert, der die zentrale Konfiguration von Sicherheitsstufen erlaubt, schotten die Systeme unter AIX 6.1 zusätzlich ab. (rh)

ANDREAS LEIBL

ist freiberuflich als Systemberater für Unix-Systeme tätig, mit Schwerpunkten auf AIX, HACMP und Linux.

Literatur

[1] Andreas Leibl; Hochverfügbarkeit; Schutzgemeinschaft; HACMP-Update: Version 5.4 für AIX und Linux; *iX* 1/2007, S. 58

[2] Andreas Leibl; Hochverfügbarkeit; Take Five; HA-Cluster mit HACMP V5 unter AIX; *iX* 3/2006, S. 96

Anwendungen sicher ausführen mit Turaya

In Sicherheit

Norbert Pohlmann, Markus Linnemann



Wegen geplanter Rechtebeschränkung auf Nutzerrechnern stieß das von Microsoft & Co. vor einigen Jahren forcierte Trusted Computing auf wenig Gegenliebe in der Öffentlichkeit. Das offene Projekt „Turaya“ will sich auf die Stärken des Konzepts konzentrieren und veröffentlicht vertrauenswürdige Pilotanwendungen.

Die Zahl der Angriffe auf Computersysteme durch Malware nimmt stetig zu. Angreifer durchbrechen die vorhandenen Sicherheitsmechanismen der Software- und Betriebssysteme wie Virenscanner und Firewalls, und es stehen zwar zahlreiche Einzelmaßnahmen, aber keine „Allzweckwaffe“ oder wirksame Strategie gegen bekannte und unbekannte Angriffe zur Verfügung. Identitätsdaten oder vertrauliche Dokumente sind ebenso gefährdet wie über die IT abgewickelte interne und externe Geschäftsprozesse.

Hier setzt Trusted Computing an. Es soll eine geräte- und netzübergreifende Vertrauens- und Sicherheitsbasis schaffen, die die Integrität aller beteiligten Rechnersysteme gewährleistet und unbefugte Zugriffe auf sie verhindert. Seit 2003 spezifiziert die Trusted Computing Group (TCG), die aus über 160 Firmen wie Sun, Intel, AMD, Microsoft, HP, IBM, Infineon, aber auch deutschen Herstellern wie Fujitsu-Siemens, Utimaco oder Sirrix besteht, diese Technologie. Die Hauptidee besteht darin, manipulationsgeschützte Sicherheitskomponenten in die Hardware zu integrieren. Sie sollen als vertrauenswürdige „Anker“ sowohl für die Integrität als auch Authentizität des Rechnersystems garantieren und softwarebasierten Angriffen entgegenwirken. Eine solche Sicherheitskomponente ist das „Trusted Platform Module“ (TPM).

Es ist ein kleiner passiver Chip, der fest mit der Systemplattform (Mainboard oder Prozessor) verbunden ist und einen Microcontroller enthält. TPMs werden von mehreren Chip-Produzenten angeboten und inzwischen in die Motherboards von Servern, Desktops und Laptops verbreiteter Marken integriert. Im Jahr 2006 waren circa 60 Millionen Einheiten im Einsatz, für 2008 rechnet die Fachwelt mit bis zu 200 Millionen.

Die Architektur des TPM ähnelt der einer Smartcard. Der Chip beinhaltet einen Krypto-Koprozessor, einen Zufallszahlengenerator und das „Platform Configuration Register“ (PCR), in das er die Hash-Werte von Konfigurationszuständen speichert. Diese Messwerte lassen sich überprüfen und machen Änderungen der Soft- oder Hardwarekonfiguration erkennbar.

Die Messung bringt es an den Tag

Sobald ein Softwareangriff oder eine Veränderung von Hardwarekomponenten die Systemkonfiguration verändert, ändern sich die Messwerte und sind dann unter Umständen nicht mehr als vertrauenswürdig einzustufen. Der Messvorgang beginnt während des Systemstarts, dem sicheren Booten. Stimmen die gemessenen Werte nicht mit den Vorgaben überein, kann eine Sicherheitsanwendung diese Information abfragen und als Reaktion beispielsweise den Bootvorgang abbrechen. So wird eine Aussage über die Vertrauenswürdigkeit eines Rechnersystems möglich.

Beim Anwendungsfall Auto würde das etwa bedeuten, dass die Werkstatt das Update eines Autosystems nur durchführen könnte, wenn sich Auto und Werkstattsystem in einer vertrauenswürdigen Systemkonfiguration befinden, definiert durch die Messwerte der Systeme.

Die Grundfunktion der Messbarkeit von Systemkonfigurationen ermöglicht es außerdem, Daten an eine solche Konfiguration zu binden. Dieses

sogenannte „Sealing“ schützt Dokumente eines Anwenders vor fremdem Zugriff. Es gewährleistet auch den Transfer eines Dokuments an ein für den Dokumentenzugriff autorisiertes anderes Rechnersystem – und nur an ein solches.

Man kann mit Trusted Computing beispielsweise den Hash-Wert einer vertrauenswürdigen Systemkonfiguration mit den zu schützenden Dokumenten zu einem Datenpaket verbinden. Die dabei eingesetzte Verschlüsselung gewährleistet, dass die Daten nur auf den Rechnersystemen wieder entschlüsselt werden können, die die definierte Konfiguration vorweisen.

Zusätzlich zum Zustand des eigenen Systems ist es hilfreich, den des Rechnersystems eines Kommunikationspartners zu kennen. Vor einem Dokumentenversand sollte man sicher sein, dass das andere Rechnersystem auch wirklich dasjenige ist, das es vorgibt zu sein, und dass es sich in einem vertrauenswürdigen Systemzustand befindet. Die „Remote Attestation“ überprüft das. Da die TPMs mit ihren Schlüsseln Einzigartigkeit gewährleisten, ist ein Rechnersystem mit Bezug auf seinen Integritätszustand eindeutig identifizierbar.

Nur abgeleitete Schlüssel verwenden

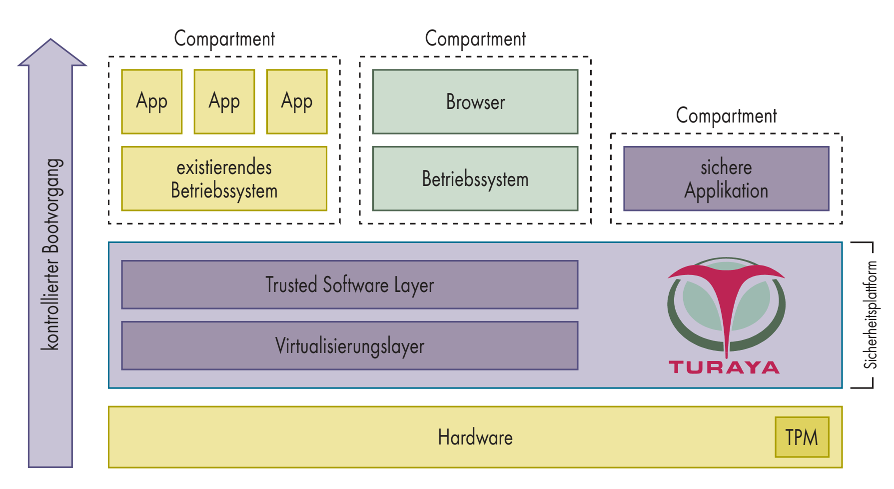
Wichtig dabei ist für die Gewährleistung des Datenschutzes, dass nie der Hauptschlüssel (Endorsement Key) des TPM verwendet wird, sondern ausschließlich abgeleitete Schlüssel. Die beteiligten Rechnersysteme übermitteln ihren Systemkonfigurationszustand an eine vertrauenswürdige dritte Instanz und weisen sich durch Schlüssel und Zertifikate ihres TPMs aus. Hat jemand die Systemkonfiguration so verändert, dass sie als nicht vertrauenswürdig gilt, wird eine Kommunikation nicht zugelassen.

Voraussetzung für das Trusted Computing ist eine Infrastrukturkomponente, die sämtliche Vorgänge der beschriebenen Anwendungen steuert. Ihre wichtigste Aufgabe besteht darin, die Integritätsprüfungen durchzuführen und auszuwerten. Das TPM allein bringt noch keine höhere Sicherheit, es ist lediglich ein passives Modul, das Sicherheitsdienste anbietet. Um es nutzen zu können, muss der Besitzer es zuerst aktivieren.

Herkömmliche Betriebssysteme können aufgrund der hohen Fehleranfälligkeit und der monolithischen Struktur den Ansprüchen an eine solche Sicherheitsplattform nicht genügen. Sie können zu einfach kompromittiert werden und vertrauenswürdige Zustände vortäuschen, die nicht den realen entsprechen. Es fehlen entscheidende Strukturen und Konzepte, die zum Beispiel eine strikte Trennung von Speicherbereichen ermöglichen, um bei einem Angriff den Schaden einzuschränken. Auch können sie bisher nicht die Authentizität von Applikationen oder des Rechnersystems gewährleisten, wodurch eine Anwendung nie einen nachweisbaren vertrauenswürdigen Status erreichen kann. Eine Sicherheitsplattform muss selbst möglichst wenig oder gar nicht anfällig für Angriffe sein.

Die Open-Source-Sicherheitsplattform Turaya wählt einen eigenen Ansatz, der die Vorteile des Trusted Computing nutzt und die Diskriminierung von Anwendern oder Anbietern verhindert. Sie wird im Rahmen des Forschungs- und Entwicklungsprojekts EMSCB (European Multilaterally Secure Computing Base, www.emscb.org) entwickelt, einem Konsortium aus dem Institut für Internet-Sicherheit der FH Gelsenkirchen, der Ruhr-Universität Bochum, der TU Dresden und den Firmen Sirrix AG und escrypt GmbH. Das Bundesministerium für Wirtschaft und Technologie fördert das Projekt und Industriepartner wie SAP AG und Bosch/Blaupunkt unterstützen die insgesamt fünf Pilotanwendungen. Ziel ist es, eine Sicherheitsplattform mit offener Architektur und Schnittstellen zu schaffen, die als Basis für vertrauenswürdige IT-Systeme dient.

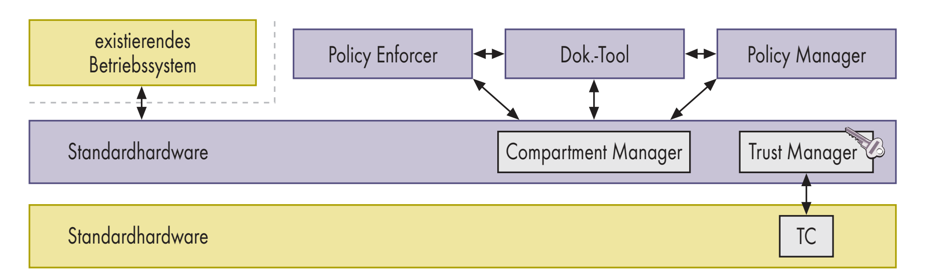
Turaya zeichnet sich durch einen modularen Aufbau, einen offenen Quellcode und eine geringe Komplexität aus. Zusätzlich bietet sie die Möglichkeit, Rechte und Regeln durchzusetzen (Policy Enforcement). Und das auf faire Art und Weise: Während für Endbenutzer Datenschutzaspekte von Bedeutung



Turaya schiebt sich als betriebssystemähnliche Sicherheitsschicht zwischen Hardware und Betriebssystem. In sogenannten Compartments kann man sicherheitsrelevante Anwendungen mit eigenem Betriebssystem oder ohne isoliert und parallel ausführen (Abb. 1).

iX-TRACT

- Da einzelne Sicherheitsmaßnahmen nicht immer greifen oder von Kriminellen außer Gefecht gesetzt werden, ist für kritische Geschäftsprozesse eine grundlegende Sicherheitsinfrastruktur erforderlich.
- Die Basis für die europäische Open-Source-Sicherheitsplattform „Turaya“ ist das Trusted Computing. Das dafür erforderliche Trusted Platform Module ist heutzutage in nahezu alle Computersysteme eingebaut.
- Kennzeichnende Eigenschaften der Sicherheitsplattform sind Betriebssystemunabhängigkeit und offengelegter Code sowie Schnittstellen, die einerseits eine Evaluierung aus Sicherheitssicht und andererseits die Nutzung für Produkte aller Hersteller ermöglichen.



Der Policy Enforcer sorgt für die Durchsetzung der vorgegebenen Richtlinien, wie Mitarbeiter mit welchen Dokumenten verfahren dürfen (Abb. 2).

sind, sind für Unternehmen und Behörden die sichere und vertrauliche Behandlung von wichtigen Daten sowie der Schutz der Urheberrechte und Lizenzen gegen unautorisierte Verbreitung und Nutzung relevant.

Um die geforderte Vertrauenswürdigkeit beim Austauschen von Daten zu gewährleisten, ist es notwendig, die Daten mit Rechten verknüpfen zu können, die auf einem fremden Rechnersystem durchsetzbar sind. Doch dürfen diese Regeln nicht mit denen des Empfängers kollidieren und zur Ausführung gebracht werden. So setzt Turaya zum Beispiel nicht nur die Regeln der Softwareanbieter durch, sondern berücksichtigt die aller Beteiligten. Außerdem ist die Sicherheitsplattform für jeden zugänglich und hard- sowie softwareunabhängig. Ein konventionelles Rechnersystem besteht aus Hardware, auf der ein Betriebssystem mit entsprechenden Applikationen arbeitet. Diese Hardware wird um ein TPM-Modul erweitert. Turaya schiebt sich als eigenständige betriebssystemähnliche Sicherheitsplattform zwischen Hardware und Betriebssystem. Die gesamte Ressourcenverwaltung, die Kontrolle über Funktionen und Prozesse im Hinblick auf TC-Funktionen sowie die Rechteverwaltung übernimmt Turaya.

Betriebssystemähnliche Zwischenschicht

Neben dem herkömmlichen Betriebssystem kann die Sicherheitsplattform mithilfe von Isolationsmechanismen und Virtualisierung weitere Betriebssysteme und Applikationen streng voneinander isoliert und parallel in sogenannten Compartments ausführen (Abb. 1). Sie können entweder reine sichere Applikationen enthalten, die an die Sicherheitsplattform angepasst wurden, oder schlanke Betriebssysteme mit Standardapplikationen. Im zweiten Fall misst Turaya das Betriebssystem zusammen mit der Anwendung, um die Unversehrtheit, sprich die Integrität nachweisen zu können. Auf diesem Wege muss man die Applikationen nicht anpassen. Die Architektur der Sicherheitsplattform ist in sich abgeschlossen und bietet Schnittstellen „nach oben“ zum Application Layer und „nach unten“ zum Hardware Layer an. Die Architektur ist in eine Hardware-, eine Sicherheits- und eine Applikationsebene unterteilt.

Fehleranfälligkeit abhängig von Codebasis

Eine Sicherheitsplattform sollte aus einer möglichst kleinen Codebasis bestehen und somit weit weniger komplex sein als etablierte Betriebssysteme. Ein herkömmlicher Betriebssystemkern besteht aus mehr als 3 000 000 Zeilen Code, Turaya dagegen aus weniger als 100 000. Das macht sie weniger fehleranfällig und erleichtert eine Validierung. Zusätzlich ermöglicht die Sicherheitsplattform, dass Anwender anderen ihre Daten zur Verfügung stellen können, zuvor aber bestimmte Bedingungen definieren, ob und in welcher Form der Empfänger sie auf seinem Rechnersystem verarbeiten darf. Der Automobilhersteller kann mit der sogenannten Security Policy zum Beispiel vorschreiben, ob jemand Dokumente anschauen und drucken oder nur anschauen darf. Um zu gewährleisten, dass die Daten gewissen Regeln folgen, muss der Anwender zusätzliche Policies an die Datenpakete binden. Aus dieser Funktion heraus ergeben sich neue Möglichkeiten für den vierten und fünften Meilenstein des Projekts, die voraussichtlich im Februar veröffentlicht und im Folgenden vorgestellt werden.

Derzeit existieren bereits drei Pilotanwendungen, die die Funktionen der Sicherheitsplattform demonstrieren:
– „Turaya.Crypt“ für Device-Verschlüsselung,
– „Turaya.VPN“, ein sicheres VPN-Modul (Zertifikatsmanagement),
– „Turaya.FairDRM“, ein faires Digital-Rights-Management-System.
In Kürze kommen die weiteren Pilotanwendungen „Turaya.ERM“ für das Enterprise-Rights-Management (Dokumentenmanagement) mit SAP sowie „Turaya.Embedded“ für den sicheren Einsatz von embedded Systemen (Automotive, Multimedia) hinzu.

Enterprise Rights Management ist eine Umschreibung für eine Vielzahl von Funktionen, die Daten über ihren gesamten Lebenszyklus schützen und mit entsprechenden Regeln versehen können. Die Automobilindustrie als Beispiel tauscht über ihre Systeme sensible Daten zwischen unterschiedlichen Standorten und Zulieferfirmen aus, um Prozesse zu erleichtern und zu beschleunigen. Der Verlust von Design-Daten würde im Rahmen von Plagiatsfällen einen hohen Schaden verursachen. ERM soll dafür sorgen, das die Design-Daten nur für einen definierbaren Personenkreis einsehbar und zu bearbeiten sind.

Bei Turaya.ERM, der vierten Pilotanwendung, soll die SAP AG als EMSCB-Partner das Problem der sicheren Verteilung von Dokumenten lösen. Dokumente kann man wie oben beschrieben durch eine Sicherheitsplattform auf Basis von Sealing- und Attestation-Funktionen an eigene und entfernte Plattformen binden und in dem Rahmen verschlüsseln.

Verteilt der Chef etwa ein Dokument in der Firma, soll es eventuell für bestimmte Personen lesbar, aber nicht druckbar sein, um eine unsachgemäße Verbreitung zu verhindern. Andere Mitarbeiter mit entsprechender Berechtigung müssen es drucken oder auch weiterleiten können, wieder anderen ist das Öffnen dagegen komplett untersagt. Firmenintern werden die verschiedenen Rechte gemäß der Stellung häufig durch Rollen abgebildet.

Dokumente sicher verwalten

Turaya kann mit einer Policy gemäß den Rollen des Identitätsmanagementssystems die jeweiligen Rechte in Bezug auf das Dokument durchsetzen – was den Schutz der Dokumente auch über die Unternehmensgrenzen hinaus gewährleisten soll. Mit dem Rights Management ist „Multilevel-Security“ verbunden. Das bedeutet, dass die als

sicherheitsrelevant eingestuften Vorgänge neben den unkritischen im herkömmlichen Betriebssystem auf demselben System parallel und streng isoliert ausgeführt werden können (Abb. 2).

Täglich genutzte Rechnersysteme sollen zunehmend miteinander kommunizieren können. So erwarten viele von einem neuen Auto mehr als einen fahrbaren Untersatz. Es soll etwa Multimediadaten für den DVD-Player der Kinder auf der Rückbank oder Navigationsdaten für die Reise ins Ausland zur Verfügung stellen.

Visionen der Entwickler und potenzielle Sicherheitsfeatures der Zukunft, etwa dass das eigene Auto den Bremsvorgang selbstständig einleiten soll, sobald der Vordermann langsamer fährt, dürfen nur mit vertrauenswürdigen Soft- und Hardwarekomponenten realisiert werden. Das gilt ebenfalls für das in Zukunft realisierbare Update, das die Werkstatt im Vorbeifahren einspielt. Danach muss sichergestellt sein, dass das Rechnersystem vertrauenswürdig ist und die Bremssysteme weiterhin funktionieren. Für diese Anwendungsfälle gibt es schon Konzepte und erste Praxistests.

Die Aufgabe besteht in der Umsetzung der beschriebenen Funktionen auf andere Systeme. Das Rechnersystem, das die Updates der Werkstatt entgegennimmt, ist ein sogenanntes eingebettetes System. Die Turaya-Plattform wird beispielsweise auf ARM-Prozessoren portiert, um diese sicher und vertrauenswürdig zu gestalten. Zu diesem Bereich gehören maschinelle Rechnersysteme ebenso wie Smartphones oder PDAs.

Für die fünfte Pilotanwendung erarbeiten die Verantwortlichen gemeinsam mit Projektpartner Bosch/Blaupunkt ein Szenario. Kartenmaterial für Navigations- oder zukünftige Multimediasysteme in Autos sind kaum durch CDs ständig aktuell zu halten, und für eine Reise ins Ausland möchte man nicht gleich die Karten von ganz Europa bezahlen. Die Anwendung zeigt, wie ein Autobesitzer Kartenmaterial „on demand“ auf eine eingebettete Systemplattform laden kann. Das Kartenmaterial wird explizit für das Rechnersystem zu entsprechenden Konditionen zur Verfügung gestellt. Dieser Vorgang ist stellvertretend für das große Einsatzgebiet im Embedded-Bereich.

Fazit

Neue Informationstechniken bedürfen einer ebenso umfangreichen wie systemübergreifenden Sicherheitslösung. Damit sich Geschäftsprozesse einfacher, effektiver und trotzdem sicher gestalten lassen, muss ein Standard für alle zugänglich und nutzbar sein.

Mit Turaya können Anwender eigene Policies definieren, ihre Netzwerkumgebung auf Vertrauenswürdigkeit hin prüfen und sensible Daten sichern. Zentrale Kriterien sind Fairness und Offenheit, damit kein Hersteller mit seinen Produkten ausgeschlossen ist. Deshalb sind sämtliche Programmierschnittstellen von Turaya und der Quellcode aller sicherheitsrelevanten Komponenten zu Evaluierungszwecken offengelegt, um die Vertrauenswürdigkeit der Implementierung zu garantieren.

Turaya ermöglicht es der Open-Source-Gemeinde, „konkurrenzfähig“ zu bleiben. Zudem bietet die Sicherheitsplattform den Vorteil, dass alle sicherheitskritischen Komponenten und Anwendungen unabhängig von „klassischen“ Betriebssystemen agieren können und damit für zukünftige plattformübergreifende verteilte Anwendungen geeignet sind. Sourcecode, Pilotanwendungen und weitere Informationen finden Interessierte auf der Website des europäischen Konsortiums: www.emscb.org. (ur)

NORBERT POHLMANN UND MARKUS LINNEMANN

vom Institut für Internet-Sicherheit an der FH Gelsenkirchen arbeiten im Turaya-Projekt mit.

Literatur

[1] Informationsfilm über Turaya: www.internet-sicherheit.de/trusted-computing-film.html

[2] N. Pohlmann, H. Reimer; Trusted Computing – Ein Weg zu neuen IT-Sicherheitsarchitekturen; Vieweg-Verlag, Wiesbaden 2008

WLAN 802.11 für (fast) alle Endgeräte

Mit ohne Kabel



Uwe Schulze

Weit über Notebooks hinaus reichen mittlerweile die Einsatzgebiete drahtloser Netze – vom WLAN-Printserver über die Profi-Kamera bis zu Spielekonsole und MP3-Player.

WLAN-Chipsätze sind heute für wenige Euro zu haben und werden von den Herstellern durch sogenannte Referenzdesigns und Entwicklerkits unterstützt, sodass sich WLAN-Funktionen in beinahe beliebige Endgeräte integrieren lassen. Klar im Trend liegen Geräte mit WLAN statt des bislang eingesetzten Ethernet-, USB- oder Firewire-Interface, seien es Drucker, Projektoren oder neuartige Endgeräte wie Streaming-Clients und Internet-Radios.

Und neue Anwendungsgebiete sind keine Domäne der Heimvernetzung. In dem Maße, in dem der Standard Ethernet proprietäre Bussysteme ablöst – etwa in der System- und Sicherheitstechnik von Gebäuden oder in der industriellen Prozesssteuerung –, wird WLAN in immer mehr Endgeräten Einzug halten [1]. Gerade Videoüberwachung stellt derzeit einen schnell wachsenden Markt dar, und die durchgehende Nutzung der IP-Technik erlaubt einfachere und schnellere Implementierungen.

Zum guten Ton

Die mit Abstand größten Stückzahlen an WLAN-Chips dürften in den nächsten Jahren in mobilen Telefonen mit VoIP (Voice over Internet Protocol) verbaut werden. Mit der zunehmenden Ablösung klassischer Telefonie durch VoIP wächst die Nachfrage nach WLAN-Telefonen – sowohl im Firmeneinsatz als auch in Privathaushalten, wo vor allem die von der Telekom vorgenommene Angebotskopplung von DSL-Anschlüssen mit einem klassischen (analogen oder digitalen) Telefonanschluss dem völligen Wegfall klassischer Telefonie noch entgegensteht. Wird diese wie geplant aufgehoben, dürfte sich VoIP im Heimbereich breit durchsetzen. Und wenn der DSL-Router bereits über Wireless LAN verfügt, können WLAN-Telefone herkömmliche DECT-Technik ersetzen.

Um einen sanften Übergang von klassischer Festnetztelefonie zu Voice over IP zu ermöglichen, bieten die etablierten Telefonhersteller Hybridtelefone an, die sowohl an den vorhandenen Telefonanschluss als auch an den Breitbandrouter angeschlossen werden. Beispiele sind das Siemens Gigaset S675 IP oder S450 IP, bei denen man auf Knopfdruck zwischen Festnetz- und IP-Telefonie umschalten kann. Interessanterweise kommuniziert das Schnurlosteil dabei nicht via WLAN, sondern weiterhin über DECT, weil so keinerlei technische Änderungen notwendig sind und die IP-Technik nur in der Ladestation implementiert wird. Diese einfache Lösung wird sicher noch einige Zeit Bestand haben – mindestens, bis sparsamere WLAN-Chips zur Verfügung stehen.

Reine WLAN-Telefone dagegen, insbesondere von einigen Netzwerkherstellern angeboten, dürften langfristig gegen Kombigeräte mit GSM und WLAN (sowie UMTS) keine Chance haben.

Unter diesem Blickwinkel bedarf WLAN-Telefonie nicht nur eines Roamings zwischen Access-Points, sondern auch einer unterbrechungsfreien Übergabe von Gesprächen zwischen VoIP und Mobilfunktechniken – also eine automatische Übergabe des Gesprächs von IP an GSM, wenn sich der Anrufer aus dem Empfangsbereich des WLAN hinausbewegt. Das wird von den Herstellern mit dem Schlagwort Fixed Mobile Convergence (FMC) beworben und steckt noch in den Anfängen. Gegenwärtig erfüllen nur etwa 5 Prozent der WLAN-/Mobilfunktelefone diese Anforderung – innerhalb von drei Jahren soll sich der Anteil aber verzehnfachen. Größte Herausforderung sind dabei nicht die Endgeräte, sondern es ist die gesamte Infrastruktur, die diese Funktionen durchgehend gewährleisten muss.

Bewegung in den Markt bringt sicherlich Apples iPhone; mit dem iPod touch versieht Apple jetzt sogar MP3-Player mit WLAN, die damit nicht nur das drahtlose Herunterladen von Audio und Video ermöglichen, sondern das Browsen im Internet. Während der



Eier legende Wollmilchsau: Die Fritzbox WLAN 720 von AVM enthält neben dem 802.11n Access Point ein ADSL2+-Modem, Ethernet-Hub, Router und DECT-Telefonanlage (Abb. 1).

Umstieg auf Voice over WLAN gegenwärtig primär im Consumer-Segment stattfindet, rechnet das Marktforschungsinstitut IDC mit einer nächsten Welle in Großunternehmen. Von den kleinen Unternehmen werden dagegen in drei Jahren erst zwei Prozent der Firmen diese Technik nutzen, so die Prognose.

Kombigeräte für die vernetzte Filiale

Im SoHo-Bereich geht der Trend zur Integration von immer mehr Funktionen in einer einzigen Box. Reine Access Points werden kaum noch angeboten; stattdessen dominieren Kombigeräte, die neben der WLAN-Funktion gleich das DSL-Modem, einen Router und einen Hub oder Switch mit mehreren Ethernet-Ports mitbringen. Die in Deutschland weit verbreitete FritzBox WLAN der Berliner Firma AVM bietet zudem eine Telefonanlage mit analogen und digitalen Telefonanschlüssen sowie DECT.

Das Siemens Gigaset SE551 hingegen vereint File- und Printserver, sodass sich über USB direkt Drucker, externe Festplatten oder USB-Sticks anschließen lassen, die alle Endgeräte im Netz nutzen können. Wer derlei Funktionen bei seinem WLAN-Router vermisst, kann aber auch separate WLAN-Printserver oder gleich einen Drucker mit WLAN-Schnittstelle nutzen.

Auch externe Speichersysteme werden zunehmend mit WLAN-Schnittstellen ausgerüstet und fungieren dann als Network Attached Storage (NAS). Entsprechende Geräte zur einfachen Einbindung ins drahtlose Netz offerieren sowohl Anbieter externer Speicherlösungen (zum Beispiel Iomega NAS 100d) als auch die Netzwerkhersteller selbst.

Während die meisten Anbieter den Router oder Access Point in den Mittelpunkt stellen und um zusätzliche Funktionen ergänzen, nähern sich einige Hersteller dem Universalgerät auch von anderer Seite: Das Freecom Data Tank Gateway etwa integriert in ein externes Speichersystem nicht nur WLAN, File- und Printserver, sondern auch gleich eine Firewall und einen Router, sodass es die Rolle der Kommunikationszentrale übernehmen kann.

Was aber, wenn ältere PCs, die keinen WLAN-Anschluss besitzen, drahtlos angebunden werden sollen? Für diese Fälle gibt es WLAN-USB-Sticks, bei vielen kleinen WLAN-Routern im Paket angeboten, sodass ein problemloses Zusammenspiel garantiert sein sollte. Da Notebooks heute praktisch immer über eine WLAN-Schnittstelle verfügen, sind WLAN-Karten im PCMCIA/PC-Card-Format überflüssig geworden; in der Geschäftswelt beliebt sind aber von den Mobilfunk-Providern angebotene Kombikarten mit WLAN, UMTS und GPRS, die die unterschiedlichen Dienste zusammen abrechnen.

Einfache WLAN-Router werden bereits für unter 100 Euro angeboten, und so verwundert es nicht, wenn die Hersteller wenig für die Entwicklung aufwenden und stattdessen lieber sogenannte Referenzdesigns der Chiphersteller (zumeist Broadcom, Marvell oder Atheros) einkaufen und nur noch mit einem eigenen Gehäuse fertigen lassen.



Router wohnzimmertauglich: Der N1 Vision von Belkin erinnert eher an einen Radiowecker als an einen WLAN-Router (Abb. 2).

iX-TRACT

- Der Preisverfall bei WLAN-Chips hat 802.11n für nahezu jedes Gerät attraktiv gemacht.
- 802.11n-WLANs verdrängen sogar Near Field Communication wie Bluetooth und IrDa.
- Auch „unwichtige“ WLAN-Teilnehmer sollten WPA-Verschlüsselung beherrschen, da sonst im WLAN Sicherheitslöcher entstehen.

So gibt es auch kaum Unterschiede bei der Performance oder grundlegenden Netzwerkfunktionen – wohl aber in der Software, Bedienung und bei Zusatzfunktionen.

WLAN-Router mit Linux

Besonders beliebt bei Unix-Experten sind einige WLAN-Router der Firma Linksys, auf denen als Betriebssystem Linux läuft. Entsprechend der Vorgabe für freie Software (Open Source) stellt der Hersteller auch die Quelltexte zur Verfügung – ebenso wie die freie Entwicklergemeinde ihre selbstgeschriebene Software (www.wrt54g.net oder www.freewrt.org). So kann der Funktionsumfang einfach erweitert und das Gerät zu einem universellen Server ausgebaut werden – nur begrenzt durch den Speicherplatz.

Genau hier hat der Hersteller aber bereits gespart, denn der früher Linux-getriebene WRT54G wird nur noch mit weniger Speicher und dem Betriebssystem VxWorks ausgeliefert. Die Linux-Fraktion kann aber auf den WRT64GL zurückgreifen. Inzwischen bieten auch andere Hersteller ähnliche Geräte mit offenem Linux-Betriebssystem an, etwa Asus sein WL-500g oder Netgear das WGT634u.

Der Preisverfall bei der Hardware hat dazu geführt, dass viele Service-Provider ein WLAN-fähiges Endgerät bei Abschluss eines DSL-Vertrages kostenlos zur Verfügung stellen. Während es sich bei den meisten Anbietern um das originale Gerät des Hardwareherstellers handelt – sodass man sich mit Supportanfragen und für Software-Upgrades direkt an diesen wenden kann –, lässt insbesondere die Deutsche Telekom OEM-Geräte im Telekom-Design entwickeln. So verbargen sich hinter der Marke Speedport der T-Com in der Vergangenheit AVM-, Hitachi- und Siemens-Geräte, derzeit aber ein asiatisches Produkt einer Tochter von Acer und Philips. Hier ist man bei Support und Software meist auf den Service-Provider angewiesen und kann sich nicht direkt an den Hersteller wenden, weil häufig an den OEM-Geräten spezielle Anpassungen vorgenommen wurden.



Gute Unterhaltung

Seit Jahren beschwören die Hersteller das Zusammenwachsen von Unterhaltungselektronik und Computertechnik. Ein einfacher Grund, der dem bisher entgegenstand, ist der, dass Bündel von Kabeln in der Wohnung längst nicht so selbstverständlich toleriert werden wie im Büro. Der Einsatz von kabellosem LAN kann hier also eine neue Chance bieten. Schon gibt es erste Fernseher mit WLAN-Schnittstelle – angeboten etwa in der Connect-Serie von Loewe –, und auf der letztjährigen Internationalen Funkausstellung in Berlin konnte man den Satelliten-Receiver SRT 6300 WRT der Firma Strong in Augenschein nehmen, der mit seinen drei WLAN-Antennen auf den ersten Blick eher an ein Netzwerk-Device erinnert als an Unterhaltungselektronik. Mit angebotenen Master- und Slave-Geräten macht sich das WLAN hier völlig unabhängig von PC oder Router.

Interessant sind auch völlig neuartige Geräte, die technisch kaum etwas mit klassischer Unterhaltungselektronik gemein haben und zwingend eine Netzwerkverbindung zu einem Server oder ins Internet benötigen – und damit prä-

Die WLAN-Kamera WVC200 von Linksys erlaubt den Zugriff von jedem Browser aus dem Internet und die Aufzeichnung des Videomaterials irgendwo im Netz (Abb. 4).

destiniert sind für Wireless LAN. Zu ihnen gehören Internet-Radios und Streaming-Clients. Erstere können bis zu zehntausend Sender aus dem Internet empfangen, und wenn dies drahtlos über WLAN erfolgt, unterscheidet es sich kaum noch von einem klassischen Radio. Streaming-Clients empfangen die gesamte Musiksammlung von der heimischen Festplatte, notwendig ist dafür in der Regel nur der Windows Media Player oder eine andere UPnP-AV-fähige Software (Universal Plug and Play Audio Video).

Auch Audio muss sicher sein

Bei Geräten, die UPnP nicht unterstützen, ist man auf die mitgelieferte Serversoftware angewiesen und kann keine Interoperabilität mit Geräten anderer Hersteller erwarten. Ferner sollte man darauf achten, dass die Clients die als sicher geltende WPA-Verschlüsselung beherrschen und nicht nur WEP – leider immer noch keine Selbstverständlichkeit, vielleicht, weil die Hersteller von Unterhaltungselektronik den Fokus auf andere Funktionen richten. Auch wenn man meinen könnte, für eine reine Audio-Verbindung sei dies nicht so wichtig, ist zu beachten, dass



Internet-Radio und Streaming-Client WAP-5000 von Teac; im Vordergrund die Fernbedienung (Abb. 3).

alle Teilnehmer im WLAN sicher kommunizieren müssen, und das geht eben nur mit WPA.

Unwichtig für Audio ist hingegen die Unterstützung neuerer (und schnellerer) WLAN-Standards, etwa 802.11n. Denn selbst für unkomprimierte Audio-Formate reicht der langsame 802.11b-Standard; MP3 stellt noch geringere Ansprüche. Erst für die Übertragung von Video werden die schnelleren WLAN-Standards interessant. Ein Video-Stream von DVD liefert etwa 10 MBit/s, also etwa die Hälfte dessen, was 802.11g zu leisten vermag. Bei ungünstigen Bedingungen in Bezug auf Entfernung und Hindernisse stößt man bereits an die Grenzen.

Übergang zur Unterhaltungselektronik

In Zeiten, da sich die heimische Plattensammlung eher auf einem MP3-Player befindet als im CD-Schrank, sind bereits alle Voraussetzungen für den Einsatz von Streaming-Clients gegeben, und wer nicht den PC starten möchte, findet auch spezielle Media-Server für das Wohnzimmer, etwa von Philips.

Sony geht hier einen anderen Weg und bietet eine Location Free genannte externe Box zur Verbindung von Geräten der Unterhaltungselektronik und PC oder Playstation über WLAN. Der Clou daran: Sie ist mittels dynamischem DNS auch aus dem Internet erreichbar, sodass etwa aus dem Hotel auf den heimischen Videorekorder zugegriffen werden kann.

Wie auch bei MP3-Playern sind die Pioniere der neuen Technologien nicht die großen Hersteller von Unterhaltungselektronik, sondern eher Spezialanbieter mit komplett neu entwickelten Geräten. Streaming über Wireless LAN ist nicht auf Audiodaten beschränkt: Der inzwischen von Linksys übernommene dänische DivX-Pionier Kiss Technology war der erste Anbieter von Mediaplayern für Video-Streaming mit WLAN-Schnittstelle; inzwischen gibt es auch Alternativen wie Buffalo mit dem Link Theater. Als Ersatz für den ständig laufenden PC bietet Buffalo einen kompakten Mediaserver an, der ebenfalls aus dem Internet erreichbar ist. Insbesondere der nächste WLAN-Standard 802.11n wird dazu beitragen, dass man Video – auch hochauflösend – ohne Abstriche drahtlos übertragen kann.



Linux-getrieben: Der WLAN-SoHo-Router WRT54GL von Linksys (Abb. 5).

Die Spielekonsolenhersteller, die ihre Geräte als Mittelpunkt der Unterhaltung sehen, setzen ebenfalls auf Wireless LAN. Die Sony Playstation 3 hat in der 60-GByte-Version eine entsprechende Schnittstelle bereits standardmäßig eingebaut, bei der Xbox gibt es den externen Adapter optional, Nintendos Wii verfügt ebenfalls über ein WLAN-Interface.

Video spielt aber nicht nur für die Unterhaltung eine Rolle, sondern auch für Überwachungskameras, die besonders davon profitieren, Wireless LAN statt Ethernet-Kabel zu nutzen, da sie oft im Außenbereich und an unzugänglichen Stellen angebracht sind. IP-basierte Videoüberwachung wird als einer der schnell wachsenden Zukunftsmärkte angesehen, da die Übertragung, Speicherung und Auswertung keine separate Infrastruktur erfordert. Alle Hersteller entsprechender Geräte unterstützen inzwischen WLAN.

WLAN ersetzt aber nicht nur den drahtgebundenen Ethernet-Anschluss in den Endgeräten, sondern zunehmend auch USB- oder Firewire-Anschlüsse, die zwar nur eine kurze Entfernung überbrücken, aber häufig an- und abgesteckt werden. Damit steht es eher in der Tradition von Infrarot- oder Bluetooth-Schnittstellen, deren Datendurchsatz zu gering ist.

Nikon war der erste Hersteller, der seine Profikamera D2H mit einer WLAN-Option ausrüstete, die Bilder ohne USB-Stecker auf den PC überträgt; inzwischen gehört WLAN bei den Profikameras schon fast zum Standard – meistens integriert in den zusätzlichen Akkugriff. So kann man die Bilder nicht nur drahtlos und schnell auf den heimischen PC übertragen; wenn man sich in Reichweite eines Hotspots befindet, sollen sich Bilder ohne einen zusätzlichen Rechner direkt ins Internet senden lassen, etwa an die heimische Redaktion, ein Fotolabor oder eine Bildergalerie.

Auch Beamer mit WLAN-Schnittstelle sind bereits auf dem Markt, so von Acer oder Panasonic. Hier wird das VGA-Kabel ersetzt, weshalb eine spezielle Client-Software auf dem Rechner zu installieren ist. Diese Prozedur kann man leider auch nicht mit einem speziellen WLAN-Projektor-Server umgehen, wie er von Lindy angeboten wird. (JS/hw)

Ortung via WLAN

Eine interessante Zusatzfunktion in Wireless LANs ergibt sich aus der Tatsache, dass die Access Points Gebäude vollständig und überlappend ausleuchten können. Somit kann man feststellen, wo sich WLAN-fähige Endgeräte befinden. Einige Hersteller bieten spezielle Hard- und Softwarelösungen an, mit denen sich Lokalisierungsservices realisieren lassen, etwa Trapeze oder Cisco mit speziellen Location Appliances oder die finnische Firma Ekahau, die sich auf komplette Lokalisierungslösungen spezialisiert hat. Damit lässt sich auf einfache Weise ermitteln, in welchem Raum und wo innerhalb des Raumes sich beispielsweise ein WLAN-fähiger Beamer oder ein WLAN-Handy befindet.

Darüber hinaus gibt es spezielle Tags (etwa von AeroScout oder PanGo), mit denen sich beliebige Geräte kennzeichnen lassen, zum Beispiel medizinische Geräte im Krankenhaus, Gabelstapler in einer Werkhalle oder Container auf einem Hafengelände. Der hierfür häufig verwendete Begriff Real Time Location Systems (RTLS) wurde ursprünglich im Zusammenhang mit RFID verwendet, inzwischen aber auch zunehmend für entsprechende Dienste auf WLAN-Basis.

Gegenüber GSM ist die Lokalisierung wesentlich genauer und gegenüber RFID ist ein größerer Abstand zu den Access Points möglich. Wenn die WLAN-Infrastruktur bereits vorhanden ist, lässt sich ein darauf basierender Lokalisierungsservice ohne zusätzliche Investitionen realisieren.

UWE SCHULZE

ist Fachautor in Berlin.

Literatur

[1] Lutz Rauchhaupt, Spiro Trikaliotis; Netztechnik; Industriefunk; WLAN und Co. im Industrieeinsatz; *iX* 12/07; S. 120

Rechtsrahmen für Unternehmen in virtuellen Welten

Verdoppelt

Tobias Haar

Unternehmen entdecken zunehmend die Bedeutung sogenannter Metaversen wie Second Life für ihre Geschäftstätigkeiten. Gleich, ob jemand dort nur einen Markenauftritt oder einen Onlineshop betreiben will, er muss sich mit den rechtlichen Aspekten beschäftigen.

Noch vor etwa 12 Jahren war es keineswegs selbstverständlich, dass Unternehmen einen Webauftritt hatten. Heutzutage sind unternehmensbezogene Internetseiten, Webshops und E-Mail-Kommunikation aus dem Geschäftsleben gar nicht mehr wegzudenken. Vieles in diesem Bereich ist selbstverständlich geworden, nicht zuletzt, weil man sich auf bestimmte Regeln verlassen darf. Geschäftlicher Erfolg kann sich auf Dauer nur dort einstellen, wo ein Mindestmaß an Rechtssicherheit herrscht. Für Juristen ist das Internet, oder wie manche schon fast abfällig dazu sagen, das Web 1.0, längst kein Neuland mehr. Mit den meisten rechtlichen Fragestellungen lässt sich ganz gut umgehen. Viele Rechtsthemen sind in der Fachwelt abschließend diskutiert oder durch Gerichte entschieden worden.

Jetzt droht neues Ungemach. Mit der zunehmenden Bedeutung des Web 2.0 und insbesondere den Metaversen scheinen sich Kommunikationstechnologien herauszubilden, die juristisch in etlichen Bereichen noch völlig im Dunkeln liegen. Mit dem stetig steigenden Interesse der Unternehmen, sich ebenfalls in diesen virtuellen Welten zu tummeln, nehmen die Fragen nach den rechtlichen Rahmenbedingungen zu. Allein die bekannteste virtuelle Welt „Second Life" verzeichnet seit ihrer Gründung im Jahr 2003 mittlerweile annähernd 7 Millionen Teilnehmer, wobei allerdings nur rund 550 000 pro Woche online sind. Noch sind es nach Angaben der Betreiberin Linden Labs nur circa 1,5 Millionen US-Dollar, die in Second Life tagtäglich umgesetzt werden. Aber immerhin. Außerdem ist die Tendenz steigend.

Mit der Bedeutung von Second Life & Co. wächst auch die Zahl der Unternehmen, die eine Präsenz in dieser virtuellen Welt aufbauen – von der Deutschen Post über IBM, Kraft, BMW bis hin zu Plus. Doch auch wer als Unternehmer keinen Geschäftsauftritt in den Metaversen plant, kommt womöglich nicht darum herum, sich mit den rechtlichen Fragen dieser virtuellen Welten auseinanderzusetzen. Wer beispielsweise davon erfährt, dass jemand ohne Lizenz für ein Unternehmen geschützte Marken in Second Life verwendet, sollte dagegen mit juristischen Mitteln vorgehen.

Entscheidend für die rechtliche Einordnung der Beziehungen zwischen den an Second Life Beteiligten ist, ob zwischen ihnen ein Vertrag besteht oder nicht. Die Ansprüche eines Unternehmens mit Second-Life-Auftritt an den Betreiber Linden Labs und umgekehrt richten sich nach dem Nutzungsvertrag, den die beiden abgeschlossen haben. Wird zwischen einem Unternehmen und einem anderen Nutzer über Second Life ein Geschäft abgeschlossen, so sind rechtliche Probleme auf der Grundlage dieses Vertrages zu klären.

In manchen Fällen existiert aber keiner. Verwendet ein Nutzer ungefragt ein Logo, eine Marke oder ein urheberrechtlich geschütztes Werk eines anderen, besteht zwischen diesen beiden gerade kein Vertrag. Dann – und gerade das sind in der virtuellen Welt die schwierigen Fälle – muss erst einmal aufwendig geklärt werden, welche Rechtsordnung zur Entscheidung über eventuelle Rechtsansprüche heranzuziehen ist. Erst wenn das feststeht, können die Beteiligten feststellen lassen, wer einen Rechtsanspruch gegen wen hat oder eben auch nicht.

Die Firma Linden Labs hat ihren Sitz in Kalifornien in den USA. Konsequenterweise schreibt sie in ihren Nutzungsbedingungen auch vor, dass die Rechtsbeziehungen zwischen den Nutzern und ihr dem kalifornischen Recht unterliegen. Schließt eine Privatperson einen Nutzungsvertrag mit Linden Labs ab, kann man noch darüber streiten, ob man es dieser rechtlich zumuten kann, nach kalifornischem Recht und womöglich vor einem kalifornischen Gericht zu klagen und verklagt zu werden.

Bei einem Unternehmen stellt sich diese Frage grundsätzlich nicht. Wer als Geschäftsmann einen englischen Vertrag abschließt, dem ist es auch zuzumuten, dass der Vertrag nach dem Recht eines anderen Staates auszulegen ist und Rechtsstreitigkeiten vor einem ausländischen Gericht – im Fall von Second Life den Gerichten in San Francisco – ausgetragen werden müssen. Das muss man wissen, denn nach kalifornischem Recht sind manche Gestaltungen in den allgemeinen Nutzungsbedingungen, den Terms of Service, möglicherweise zulässig, die nach deutschem Recht undenkbar wären. So behält sich Linden Labs zum Beispiel das Recht vor, jederzeit die Nutzungsbedingungen nach eigenem Ermessen zu ändern. Die Änderungen wiederum muss das Unternehmen dem Nutzer nicht einmal mitteilen, es genügt vielmehr, dass es sie auf seinen Webseiten veröffentlicht.

Hier regiert die Willkür

Geld regiert auch die virtuelle Welt von Second Life. Aber Vorsicht, denn Linden Lab hat nach den Nutzungsbedingungen jederzeit das Recht, die Linden-Dollar zu entwerten, zu reglementieren oder gar abzuschaffen. Interessant ist, dass ausdrücklich ein Recht vorgesehen ist, weitere Linden-Dollar in Umlauf zu bringen. Sie sind damit nicht vor einer durch Linden Labs betriebenen Inflation geschützt. Wer seine Geschäfte in dieser Währung abschließt, muss also stets darauf achten, den richtigen Zeitpunkt des Rücktausches in echte US-Dollar nicht zu verpassen.

Wer eine Unternehmenspräsenz in Second Life aufbaut und zu festen Öffnungszeiten sein Geschäft offenhalten möchte, muss berücksichtigen, dass der Betreiber nahezu jederzeit den Service für Wartungsarbeiten unterbrechen kann. Hart ist auch, dass Linden Labs „aus jedem Grund oder grundlos“ einen Nutzer-Account sperren oder löschen darf, ohne dass ein Anspruch auf finanziellen Ausgleich hierfür besteht. Gerade diese Klausel ist derzeit Gegenstand einer Klage gegen Linden Labs in Kalifornien. Ausgang offen.

Urheberrecht adieu

Was die Schaffung urheberrechtlich geschützter Werke in der virtuellen Welt anbelangt, soll Linden Labs nach den Nutzungsbedingungen berechtigt sein, diese jederzeit etwa für Marketingzwecke nutzen zu können. Daneben darf der Betreiber jederzeit sämtliche durch Nutzer geschaffene Werke löschen – mit oder ohne Grund. Interessant ist auch, dass Linden Labs sich das Recht vorbehält, Streitigkeiten zwischen Nutzern zu schlichten, sich hierzu aber nicht verpflichtet sieht. Fast naiv aus juristischer Sicht klingt die Klausel, dass solche Streitschlichtungen zwar für die virtuelle Welt von Second Life abschließend sind, aber nicht in der realen Welt gelten.

Während die Rechtsbeziehungen zum Betreiber teilweise vielleicht unfair, aber zumindest einigermaßen klar, weil schriftlich niedergelegt, sind, wird es bei Vertragsabschlüssen mit Kunden in der virtuellen Welt schon deutlich schwieriger. Die Probleme fangen damit an, dass man ja nicht weiß, mit wem man es zu tun hat. Die Nutzer agieren grundsätzlich unter Pseudonymen, durch die man kaum auf die reale Person schließen kann. Bei einem normalen Geschäft Geld gegen Ware wird in den meisten Fällen alles glatt gehen, denn die Identität des Vertragspartners spielt häufig keine Rolle. Wenn aber nicht, könnte es schwierig sein, Linden Labs zur Herausgabe der wahren Personendaten des Vertragspartners zu bewegen. Vielleicht auch aus diesem Grund „locken“ Unternehmen mit einem Auftritt in Second Life die Besucher ihrer Shops im Metaversum auf ganz normale Webseiten und Onlineshops im Internet.

Wer wie die bekannt gewordene Second-Life-Dollarmillionärin Ailin Gräf geschäftlichen Erfolg in einer virtuellen Welt haben will, muss auch ein paar Gedanken an die steuerrechtlichen Regeln verschwenden. Bislang gibt es zu dieser Thematik noch keine befriedigende Antwort der staatlichen Steuerbehörden. Sind Linden-Dollars steuerfrei? Vermutlich nicht, aber konkrete Aussagen dazu gibt es nicht. Spätestens dann aber, wenn ein Nutzer sie wieder in US-Dollar zurücktauschen möchte, will der Fiskus zugreifen.

Was aber, wenn die Linden-Dollars einfach gar nicht zurückgetauscht werden? Was, wenn der Nutzer seine Linden-Dollars in Steuerparadiesen auslöst oder zu Zwecken der Geldwäsche von einem Land in ein anderes verschiebt und dort umtauscht? Es wird sicher noch einige Zeit dauern, bis die Steuerbehörden in den verschiedenen Ländern darauf abschließende Antworten gefunden haben. Auch beim Internet hat es einige Zeit gedauert, bis die staatlichen Stellen Regelungen zur Besteuerung von Geschäftsabschlüssen im Web erlassen hatten. Bis es soweit war, gab es in vielen Ländern ein ausdrückliches Steuer-Moratorium, das die Transaktionen von der Besteuerung befreite und somit für Rechtssicherheit sorgte. Soweit ist es bei den Metaversen aber noch nicht.

Mangels einer staatlichen Ordnung in der virtuellen Welt – für viele gerade der Grund, sich dort aufzuhalten – drohen Unternehmen andere Gefahren, gegen die es in der realen Welt meist einigermaßen verlässliche Mittel gibt. So ist man letztlich vom Wohlwollen von Linden Lab abhängig, wenn es etwa zu einer Schutzgelderpressung durch einen anderen Nutzer der virtuellen Welt kommt. Folgt man solchen Forderungen nicht, drohen codegesteuerte Angriffe gegen die eigene Präsenz in Second Life. Ähnlich erging es dem amerikanischen Fernsehsender ABC bei einem der ersten „Terroranschläge in Second Life“, bei dem dessen Unternehmsauftritt auf einer Insel durch ein Script völlig zerstört wurde. Zwar versetzten die Betreiber die Insel wieder in den Ursprungszustand zurück, einen Rechtsanspruch hätte ABC darauf aber nach den Nutzungsbedingungen nicht gehabt.

Für Unternehmen mit einem eigenen Auftritt in Metaversen stellen sich weitere wesentliche Fragen. Müssen die Geschäftsauftritte deutscher Unternehmen mit dem deutschen Recht in Einklang stehen? Wenn dem so ist, müssen sie die Regelungen zum Fernabsatz (einschließlich der grundlosen Rückgabemöglichkeit), zur Impressumspflicht, zur Haftung für Inhalte et cetera beachten. Wer sich hier am deutschen Rechtsrahmen orientiert, ist wahrscheinlich juristisch auf der sicheren Seite – zumindest wenn er deutschsprachige Angebote erstellt. Insofern dürfte nichts anderes gelten als bei einem „normalen“ Internetauftritt.

Ein spannendes Thema dürfte sein, wie Gerichte die Haftung der Betreiber von Metaversen beurteilen. Haftet Linden Lab etwa entsprechend den Regeln, die der deutsche Gesetzgeber und die Gerichte hierzulande für Beiträge in Meinungsforen oder für rechtswidrige Auktionen in Online-Aktionshäusern aufgestellt haben? Muss Linden Lab als globaler Anbieter jede Rechtsordnung der Welt beachten? Ein interessanter Vorschlag diesbezüglich stammt vom Betreiber von Second Life selbst: Er schlägt vor, ein Filtersystem aufzubauen, mit dem einzelne Staaten ihr nationales Recht in Second Life umsetzen können. Zugriffe auf Second Life aus einem Staat heraus müssten also zuerst durch den jeweiligen nationalen Filter freigegeben werden. Ein kaum praktikables und wenig wünschenswertes Vorhaben staatlicher Zensur und inhaltlicher Vorabkontrolle.

Fazit

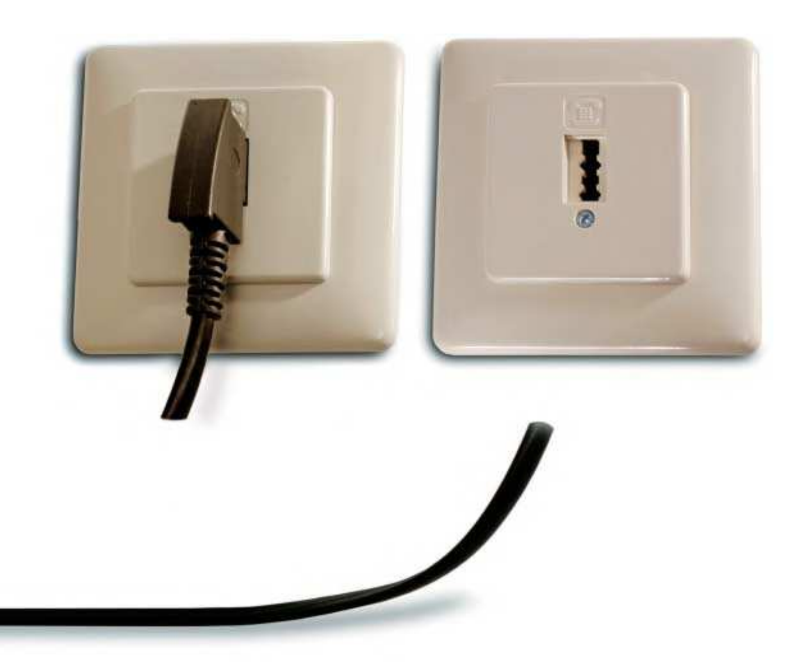
Eine gewisse Vorsicht ist angebracht, wenn Unternehmen ihre Geschäftstätigkeiten auf die virtuelle Welt ausweiten. Zwar sind die meisten juristischen Probleme letztlich lösbar. Schwierigkeiten bereitet aber noch, seine Ansprüche gegen andere Nutzer effektiv durchzusetzen. Gerade wenn es um Rechtsverletzungen außerhalb von Vertragsbeziehungen geht, beispielsweise bei einer Markenverletzung, ist man auf den Betreiber und gegebenenfalls auf Hilfe ausländischer staatlicher Stellen angewiesen, um an die echten Daten eines anderen Nutzers zu gelangen.

Jede Investition in ein Metaversum sollte auch deswegen mit Bedacht erfolgen, weil die Nutzungsbedingungen der Betreiber häufig einseitig sind und den Nutzern im Zweifel keinen ausreichenden rechtlichen Schutz bieten. Für Juristen ist spannend, wie sich die rechtliche Diskussion um virtuelle Welten weiterentwickeln wird und wie die ersten Gerichtsurteile ausgehen werden. Ein bisschen ist es so wie am Anfang des Internetzeitalters. Aber eben nur ein bisschen. (ur)

TOBIAS HAAR, LL.M.,

ist Rechtsanwalt mit Schwerpunkt IT-Recht.





Technik und Bürokratie aktueller DSL-Angebote

Abgeschnitten

Manuel Schmitt

Das derzeitige DSL-Tarifangebot gleicht einem Dschungel, in dem Kunden besonders beim Anbieterwechsel häufig die Orientierung verlieren. Ein Blick hinter die Technik-Kulissen hilft, Ärger besonders beim Anbieterwechsel zu vermeiden.

Zum Jahresende hat die DSL-Branche wie üblich Goldgräberstimmung verbreitet. Printmedien, Radio und Fernsehen bewarben eine Unmenge von Angeboten. Doch so mancher auf diese Weise überzeugte Neukunde wartet seit Wochen auf den Wechsel oder steht gar ganz ohne Anschluss da. Gerade ein Anbieterwechsel erfordert es, sich frühzeitig über die Risiken zu informieren und den Ablauf so zu gestalten, dass es möglichst keine „Auszeit“ gibt.

Die unzähligen DSL-Angebote unterscheiden sich hinsichtlich der Technik und damit der möglichen Komplikationen stark voneinander. Die Auswahl reicht vom „originalen“ Telekom-DSL über eigene Anschlüsse (über)regionaler Alternativanbieter bis zu Komplettpaketen der großen Telekom-Konkurrenten.

Im Jahre 1999 begann die Deutsche Telekom damit, ihr damals „T-DSL“ (inzwischen T-Home DSL) getauftes Produkt in Zusammenarbeit mit ihrer Tochterfirma T-Online anzubieten. Auch wenn sich die Produkte in puncto Übertragungskapazität und eingesetzter ADSL-Technik heute stark davon unterscheiden und sowohl Konzern- als auch Produktnamen diverse Wandlungen durchgemacht haben, herrscht seit jeher eine klare Gewaltenteilung: Die Telekom stellt den eigentlichen DSL-Anschluss bereit, T-Online, den Internet-Zugang, E-Mail-Adressen et cetera.

Egal, bei wem jemand DSL-Kunde ist, er kommt an der Telekom als eigentlicher Anschluss-Eigentümerin kaum vorbei. Im September 2007 stellte der Quasi-Monopolist etwa 11,6 Millionen DSL-Anschlüsse in Deutschland bereit, was einem Marktanteil von deutlich mehr als 40 % entspricht.

Diese marktbeherrschende Stellung begründet die Regulierung durch die Bundesnetzagentur (www.bundesnetzagentur.de). Die reguliert primär zwei Dinge: Das Überlassen der sogenannten Teilnehmeranschlussleitung (TAL, auch „letzte Meile“ genannt) sowie das Bereitstellen eines Bitstrom-Zugangs („Zuführung für ISPs“, ZISP) an andere Anbieter. Nicht reguliert hingegen ist das Produkt „T-DSL Resale“.

ZISP oder die Macht über den Anschluss

Im Rahmen des ZISP-Prinzips muss die Telekom ihre DSL-Anschlüsse anderen Anbietern zur Verfügung stellen, die in der Regel weder über eine eigene letzte Meile bis zum Endkunden noch selbst über Technik in allen Vermittlungsstellen verfügen. Technisch gesehen muss die Telekom zu diesem Zweck dem Konkurrenten den DSL-Datenverkehr aller Kunden konzentriert übergeben, derzeit an 73 ZISP-Standorten deutschlandweit. Die Unterscheidung, welcher ZISP-Kunde welchen Endkunden-Datenstrom erhält, erfolgt anhand eines fixen Bestandteils („Realm“) in der Benutzerkennung bei der DSL-Einwahl, etwa nach dem Muster „kundennummer@example.com“.

Ab dem ZISP-Standort beginnt die Verantwortung des Alternativ-DSL-Anbieters. Ihm obliegt es, dem Endkunden seinen eigenen IP-Backbone zur Verfügung zu stellen, ihn zu authentifizieren, zu autorisieren und ans Internet oder bei Bedarf auch an private Netze (etwa für die interne Vernetzung von Firmenstandorten) anzuschließen. Die DSL-Tarifierung sowie die vertragliche Gestaltung sind ebenfalls dem ZISP-abhängigen Anbieter überlassen. Um seine Produkte auf der Telekom-Plattform anbieten zu können, muss der Endkunde daher zwingend einen T-DSL-Anschluss besitzen, er bleibt hierzu alleiniger Vertragspartner der Telekom und zahlt auch direkt an sie. Alle technischen Störungen des Anschlusses muss der Endkunde direkt mit der Telekom aushandeln. Nicht selten helfen aber die DSL-Anbieter dabei, auch wenn sie nicht über mehr technische Möglichkeiten oder Kontakte verfügen als der Endkunde selbst.

Im Rahmen von ZISP stellt die Telekom immer noch einen wesentlichen Teil der Technik bereit. Das beginnt bei der DSL-Dose beim Kunden, geht über die letzte Meile zum Hauptverteiler (HVT, oft auch als „Vermittlungsstelle“ bezeichnet) und die DSL-Anschlussmodule (DSLAM) bis hin zum Konzentratornetz und den 73 ZISP-Standorten.

Die Regulierung sieht bei ZISP einzig und allein eine volumenabhängige Abrechnung zwischen Telekom und dem ZISP-Kunden vor. Sie erfolgt auf Basis der von der BNetzA vorgegebenen und viel diskutierten „Peak-Load-Formel“. Anbieter, die ZISP nutzen, müssen nach dieser Formel im günstigsten Fall pro GByte, Kunde und Monat etwa 20 Cent netto berappen. Preisnachlässe, auch bei größeren Volumina, gibt es aufgrund der Regulierung nicht.

Gerade kleinere DSL-Anbieter können es kaum bewerkstelligen, den Datenstrom an bis zu 73 Standorten bundesweit „abzuholen“ – ohne eigenen, weitverzweigten IP-Backbone ein Kostengrab. Die Telekom bietet daher ein hauseigenes, auf ZISP aufbauendes Produkt namens „ISP-Gate“ an, bei dem sie die Datenströme der 73 ZISP-Standorte sammelt und dem Kunden an dessen Standort gebündelt übergibt. Dieses Produkt ist unreguliert und der Preis für andere Anbieter ist daher stark verhandlungsabhängig. Auch andere Telekommunikationsanbieter mit großen eigenen Netzen haben erkannt, dass sich hier ein enormer Markt auftut, und frühzeitig investiert. Unter anderem bieten Telefonica und QSC vergleichbare, ebenfalls unregulierte Produkte an.

Aus Endkundensicht ändert sich bei dieser ZISP-Untervariante nichts. Der DSL-Anschluss kommt weiterhin direkt von der Telekom, mitsamt Rechnungsstellung durch sie. Der DSL-Anbieter zahlt die gesamten Gebühren für die Zuführung des eigentlichen ZISP von der Telekom sowie für die Zuführung des Datenstroms zu ihm direkt an den von ihm beauftragten Dienstleister, etwa Telefonica oder QSC. Abgerechnet wird auch hier nach der originalen ZISP-Peak-Load-Formel, allerdings mit einem entsprechenden Aufschlag. Üblich sind Preise von umgerechnet etwa 30 bis 70 Cent pro GByte, Kunde und Monat, je nach abgenommenem Gesamtvolumen. Günstiger als das „originale“ ZISP wird es keinesfalls.

Ob ein Provider versucht, Kunden über Qualität oder mit juristisch-vertraglichen Maßnahmen zu halten, ist jedem Unternehmen selbst überlassen. Im DSL-Markt gibt es zumindest für letztere Variante ein hervorragendes Mittel, DSL-Endkunden an den Anbieter zu binden: einen T-DSL-Resale-Anschluss. Das Prinzip ist simpel: Nicht der Endkunde bezieht den eigentlichen T-DSL-Anschluss von der Telekom, sondern der DSL-Anbieter. Für ihn hat dieses Modell entscheidende Vorteile.

Zwischen Kundenbindung und -fesselung

Zum einen ist der DSL-Anbieter der alleinige Vertragspartner der Telekom. Er kann und muss alle vertraglichen und technischen Angelegenheiten direkt mit der Telekom aushandeln. Gerade bei Störungen hat der Endkunde demnach keine Chance, direkt mit der Telekom zu kommunizieren oder das Verfahren zu beschleunigen.

In der Regel ist der Kontakt zwischen DSL-Anbieter und Telekom nicht schlecht, zumindest besser als der zwischen Endkunde und Telekom. Es mangelt jedoch nicht an Mutmaßungen, dass Störungen von Resale-Endkunden-Anschlüssen geringere Priorität genießen als diejenigen von direkten Telekom-Kunden, etwa weil die Telekom an Resale-Anschlüssen weniger verdiene als an direkten Endkunden. Der Fairness halber sei angeführt, dass die Telekom durch Resale-Anschlüsse auch weniger Aufwand hat; unter anderem fällt der gesamte Endkunden-Service weg, Störungsmeldungen sind meist durch den Wiederverkäufer vorgefiltert, und es findet eine nicht unerhebliche Massenabnahme statt. Somit sollte sich der Nachteil wieder relativieren.

Als weiterer Vorteil eines T-DSL-Resale-Anschlusses ergibt sich für den Anbieter, dass er den Endkunden-Preis selbst gestalten kann. Er kann den Anschluss losgelöst durchaus günstiger weiterverkaufen, aber auch, und das ist die derzeit gängige Praxis, kombiniert mit dem hauseigenen Onlinetarif, meist einer Flatrate. Für Anbieter haben Kombi-Produkte erhebliche Vorteile. Endkunden haben keine Möglichkeit, den Preis klar auseinanderzudividieren, was gerade in Zeiten geringer DSL-Flatrate-Margen den Wiederverkäufern hilft, querzufinanzieren. Verluste beim Flatrate-Geschäft lassen sich durch einen zusätzlichen Anschluss-Gewinn wettmachen.

Derzeit machen T-DSL-Resale-Anschlüsse etwa 30 % aller Telekom-DSL-Anschlüsse aus. Sie unterscheiden sich technisch gesehen nicht von ihren Geschwistern, insbesondere können die Reseller keinen höheren Durchsatz oder andere Leistungsmerkmale als die Telekom selbst anbieten, da dieselbe Technik (die der Telekom) zum Einsatz kommt, insbesondere auch nicht in Bezug auf die Entbündelung von Telefon- und DSL-Anschluss. Beide Varianten setzen einen Telefon-Anschluss zwingend voraus. Auch gibt es keine Unterschiede bei der Nutzung von ZISP. Somit handelt es sich bei T-DSL Resale um ein rein kaufmännisch-vertragliches Produkt.

Welche Art von T-DSL-Anschluss der Endkunde auch immer benutzt, eins haben alle gemeinsam: Er kann mit jedem DSL-Anschluss die Online-Zugangsdaten jedes Onlineanbieters der T-DSL- respektive ZISP-Plattform nutzen.

iX-TRACT

- Mit der Marktliberalisierung in der Telekommunikation wächst die Vielfalt an DSL-Anbietern und -Anschlussvarianten.
- Provider-Wechsel bergen aufgrund fehlender Standards und Zeitvorgaben diverse technische und administrative Fallstricke und können sich unvorhersagbar lange hinziehen.
- Wechselwillige Kunden sollten einen kompletten Neuanschluss mit nachträglicher Rufnummernportierung in Betracht ziehen, wollen sie das Risiko minimieren, zeitweise ganz ohne Telekommunikation auskommen zu müssen.

So ist beispielsweise die DSL-Flatrate eines T-DSL-Resale-Anbieters technisch nicht an den von ihm bereitgestellten DSL-Anschluss geknüpft.

Gerade für kleinere DSL-Anbieter, die sich mit besonderen Features auf dem Markt positionieren, bringt dies entscheidende Vorteile. Sie können ihre Kunden unabhängig von deren Anschlussart versorgen. Wenig bekannt ist die Tatsache, dass der DSL-Anbieter nicht wissen muss, von welchem (Telefon-)Anschluss aus die Einwahl erfolgt (er erfährt es beim ZISP-Modell auch gar nicht). Dafür ist die Bitstrom-Zuführung verantwortlich, gegebenenfalls gebündelt durch ein anderes Produkt.

Somit bietet die T-DSL-Plattform mitsamt ihrem Ableger T-DSL Resale wohl die größtmögliche Flexibilität für Endkunden: Im Fall der Fälle kann er jederzeit auf einen beliebigen anderen Onlineanbieter zurückgreifen, etwa wenn das IP-Netz des eigenen Anbieters ständig unter Störungen leidet. Das Eingeben anderer Zugangsdaten im Router genügt. Es gibt zwar kaum noch DSL-by-Call-Angebote auf dem Markt, aber gerade in solchen Fällen sind sie oft die letzte Hoffnung.

Ebenfalls wenig bekannt ist, dass der Endkunde sogar mehrere DSL-Anbieter gleichzeitig nutzen kann, sprich er kann auf einem DSL-Anschluss mehrere Online-„Einwahlen“ halten. Die Übertragungskapazität des Anschlusses vervielfacht sich dadurch jedoch nicht, sie hängt von HVT und DSLAMs ab und nicht etwa vom Onlineanbieter.

Dank wachsender Anstrengungen in Sachen Kundenbindung drängen in den letzten Monaten vermehrt Komplettangebote auf den Markt. Man könnte meinen, dass es sich dabei in der Regel um T-DSL-Resale-basierende Angebote handelt. Dies ist in der Praxis jedoch nur noch selten der Fall.

Seit der Liberalisierung des Telefon- und DSL-Marktes sind Anbieter mit „beträchtlicher Marktmacht“ verpflichtet, die letzte Meile anderen Anbietern zur Verfügung zu stellen. Den Preis dafür hat die Bundesnetzagentur zuletzt im März 2007 auf 10,50 Euro netto gesenkt.

Somit kann jeder andere Anbieter die letzte Meile von der Telekom zu einem fix kalkulierbaren Betrag mieten und damit beliebige eigene Produkte anbieten, die sich technisch von denen der Telekom komplett unterscheiden können, da in diesen Fällen meist keine Telekom-Technik und -Produkte zum Einsatz kommen.

Unwägbarkeiten für Anbieter, die eine TAL anmieten, bringen jedoch die Investitionskosten mit sich. Sie müssen in jedem HVT, an dem die angemieteten Leitungen zu ihren Kunden beginnen, eigene Infrastruktur bereitstellen. Die Kosten sind je nach Standort sehr unterschiedlich. In der Regel muss ein Anbieter für die Erschließung eines jeden HVT mit Kosten in sechsstelliger Höhe rechnen. Derzeit gibt es in Deutschland etwa 8000 HVT.

Wie bei ZISP haben einige große Telekommunikationsanbieter an dieser Stelle in der Vergangenheit offenbar rechtzeitig die richtigen Schritte eingeleitet. Sie bieten, ähnlich wie bei ZISP, Zuführungs- und darüber hinausgehende Dienste für alternative Telefonie- und DSL-Anbieter auf Basis der von der Telekom gemieteten TAL bei einem Teil der HVTs in Deutschland an. Die Abdeckung schwankt von einigen Hundert bis zu einigen Tausend HVTs, je nach Anbieter. Darauf können Produkte ähnlich dem T-DSL-Resale-Anschluss basieren, aber auch entkoppelte Angebote von DSL und Internet-Telefonie, jedoch ohne klassischen Analog- oder ISDN-Anschluss. Oft stellen solche Anbieter dem eigentlichen Endkunden-Vertragspartner die gesamte Technikpalette zur Verfügung, oft auch inklusive der nötigen VoIP-Technik samt Gateways zwischen VoIP und dem herkömmlichen Telefonnetz.

Derlei Komplettangebote bieten Endkunden den enormen Vorteil, dass sie ein Produkt aus einer Hand bekommen. Ihr Anbieter ist für die komplette Realisierung verantwortlich, sie haben eine Rechnung und müssen im Störungsfall nur einen Anbieter behelligen. Darüber hinaus stimmt der Preis. Der Anbieter selbst kann mit fixen Kosten für die TAL rechnen, und die Kosten für den Internet-Datentransfer kann er anhand praxisnaher Berechnungsmethoden kalkulieren (anders als bei ZISP). Nur so lassen sich Endkunden-Preise ab etwa 20 Euro pro Monat inklusive MwSt. für Telefon- und DSL-Anschluss samt Festnetztelefonie- und DSL-Flatrate realisieren. Selbst bei denkbar kleiner Marge sind mit entsprechender Masse ansehnliche Summen zu verdienen.

Auch aus Anbietersicht bieten Komplettpakete natürlich einige Vorzüge, unter anderem die stärkste Kundenbindung, denn es gibt für die Kunden kaum einen Ausweg. Sie können in der Regel nur die Online-Zugangsdaten dieses einen Anbieters nutzen, und wenn es einmal „kracht“, bieten ihnen auch andere DSL-Zugangsdaten, etwa für DSL-by-Call, keine Alternative.

Tücken des Wechsels

Solange alles funktioniert, hat jedes Modell seine Vorzüge, kaufmännisch, technisch oder beides. Wer zu einem für die eigenen Bedürfnisse besser geeigneten oder einfach günstigeren Anbieter wechseln möchte, sollte sich lange im Voraus umfassend über Fallstricke und Besonderheiten informieren. Je nach altem und neuem Anbieter besteht die Gefahr, eine Weile ohne Telefon- oder Internet-Anschluss auskommen zu müssen.

Die wenigsten Komplikationen birgt ein Wechsel von einem T-DSL-basierten reinen Onlineanbieter zu einem anderen – wenn dabei der DSL-Anschluss weiterhin direkt von der Telekom kommt. Wenn sich weder am Telefon-

Anschluss-Varianten

T-DSL-Anschlüsse kommen direkt von der Telekom. T-DSL bietet die größtmögliche Verfügbarkeit in Deutschland. Kunden haben die freie Wahl eines Onlinetarifs und sind nicht an den Anbieter des DSL-Anschlusses gebunden.

Ein **T-DSL-Resale-Anschluss** bietet technisch gesehen dieselben Möglichkeiten wie ein T-DSL-Anschluss, allerdings oft zu einem günstigeren Preis. Nicht selten ist in einem Paketpreis der DSL-Anschluss mit der DSL-Flatrate gekoppelt. Bei Bedarf, etwa bei Störungen im IP-Netz eines Anbieters, kann man dennoch den Onlineanbieter frei wählen.

Der **Komplett-Anschluss auf Basis der „letzten Meile“ (TAL) der Telekom** bietet oftmals den günstigsten Preis. Telefon- und DSL-Anschluss realisiert ein Anbieter mit eigener Technik (bis auf die TAL). Im Paketpreis sind meist alle Grundgebühren mitsamt Flatrates für DSL und Telefonie ins Festnetz enthalten. Der Wechsel zu oder von dieser Variante birgt nicht selten Fallstricke und das Risiko, dass Kunden eine Zeit lang keinen Anschluss haben.

Komplett-Anschlüsse regionaler Anbieter mit eigenen Leitungen bieten eine hohe Flexibilität bei den angebotenen DSL-Produkten. Oft sind dank neuerer und besserer Netzinfrastruktur deutlich höhere Brandbreiten als bei Telekom-TAL-Anschlüssen möglich. Ein Wechsel zu einem anderen Onlineanbieter ist meist aufgrund der Monopolstellung des lokalen Anbieters unmöglich. Verfügbar sind solche Produkte meist nur in großen Städten.

noch am DSL-Anschluss etwas vertraglich oder technisch ändert, ist der Kunde auf der sicheren Seite. Er sollte in der Kündigung an den alten Anbieter allerdings in jedem Fall erwähnen, dass der Anschluss bestehen bleiben soll und nicht Bestandteil der Kündigung ist, insbesondere, wenn es sich beim bisherigen Anbieter um T-Online handelt.

Schnell hat man Telekom mit T-Online verwechselt, und die Kündigung landet im falschen Haus. Wer sichergehen will, sollte die neuen Zugangsdaten bereits einmal ausprobiert haben, dann kann fast nichts mehr schiefgehen. Knifflig wird es allerdings, wenn man von einem T-Home-Komplettangebot zu einem reinen T-DSL-Anschluss zurückwechseln will. Dann gilt es, die Vertragsbedingungen genau zu studieren.

Wer von einem T-DSL auf einen T-DSL-Resale-Anschluss umsteigen will, genießt meist den Service des neuen Anbieters, der einem den kompletten Vorgang abnimmt. Er informiert den alten Anbieter über die Kündigung und lässt den Anschluss auf sich selbst umschreiben. So gesehen ändert sich hier nur eine vertragliche Komponente, sprich der Leistungsnehmer wechselt. Da sich dabei der Telefon-Anschluss, genauer gesagt dessen Leistungsnehmer nicht ändert, funktioniert diese Richtung des Wechsels in der Regel gut.

Die Erfahrungen beim (Zurück-) Wechseln von einem T-DSL-Resale-Anschluss auf einen reinen T-DSL-Anschluss oder gar einen anderen T-DSL-Resale-Anschluss zeigen aber ein anderes Bild. Beiträgen in diversen Foren zufolge bestehen offenbar (technische oder administrative) Kommunikationsdefizite, die dazu führen können, dass man für einige Tage, in einzelnen Fällen sogar Wochen oder Monate ohne DSL-Anschluss dasitzt. Endkunden können hier prophylaktisch wenig tun. Wer ganz sichergehen will, sollte sich überlegen, einen weiteren Telefon-Neu-Anschluss mit „frischem“ DSL zu buchen und dessen Schaltung und die Kündigung des alten Anschlusses samt DSL entsprechend terminlich mit ausreichend Puffer zu koordinieren. Es bleibt dann allerdings die Hürde, die Rufnummer(n) später zum neuen Telefon-Anschluss mitzunehmen oder zu tauschen. Es gilt also, sich rechtzeitig mit der Telekom in Verbindung zu setzen, um dies rechtzeitig zu klären.

Ähnliches gilt für den Wechsel von einem T-DSL- oder T-DSL-Resale-Produkt auf ein Komplettangebot, das lediglich die TAL der Telekom nutzt. Mittlerweile haben sowohl Arcor als auch Telefonica, die zu den größten TAL-Anmietern zählen, bei der Bundesnetzagentur ein Missbrauchsverfahren gegen die Telekom eingeleitet. Besonders beim Anbieterwechsel dauere es oft Wochen oder gar Monate, bis die Leitungen umgestellt seien.

Tücken birgt bei dieser Form des Wechsels, dass nicht nur der DSL-, sondern auch der Telefon-Anschluss portiert wird. Kunden laufen daher Gefahr, plötzlich ganz ohne elektronische Kommunikation dazustehen, wenn sie keinen hilfsbereiten Nachbarn in WLAN-Reichweite haben. Wer sichergehen will, sollte sich auch in diesem Fall überlegen, einen komplett neuen Anschluss zu beantragen, und erst nach dessen Schaltung die alten Rufnummern manuell zu portieren.

Wer sich mit den technischen Hintergründen der DSL-Landschaft befasst, verbessert seine Chancen auf objektive Marktinformationen vor einem Anbieterwechsel deutlich und kann dem alten und bei Bedarf dem neuen Anbieter bei Abwicklungspannen wirkungsvoller begegnen.

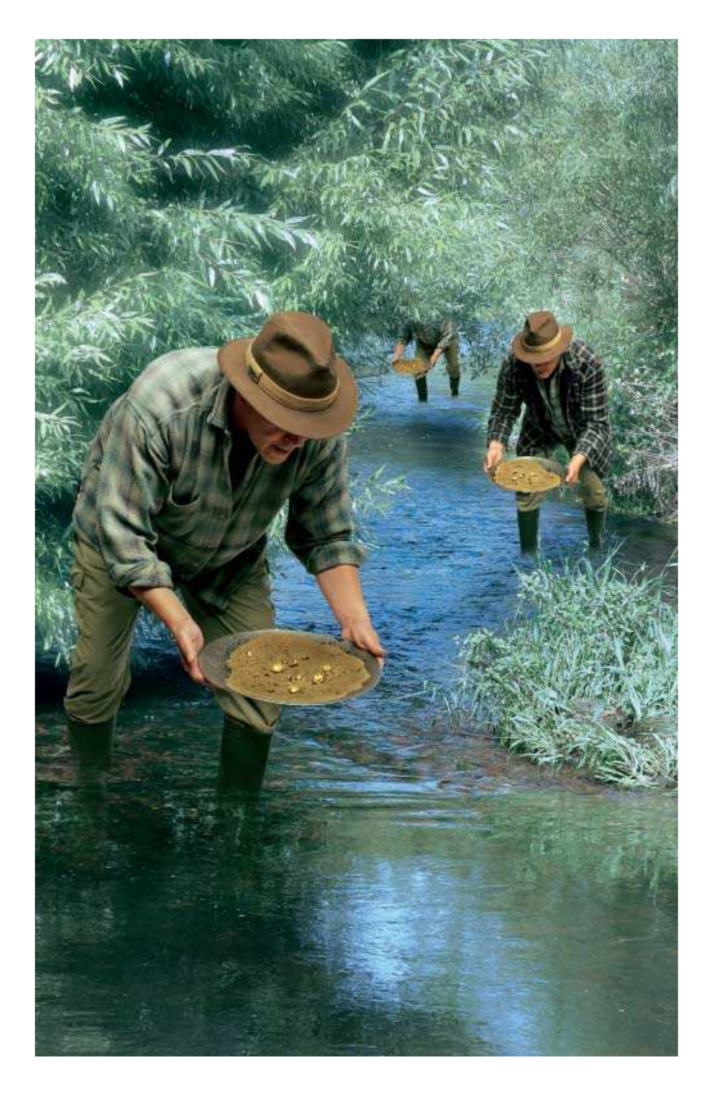
DSL-Kunden, die den Anbieter wechseln möchten, sollten sich unbedingt vor dem ersten vertraglichen Akt genau über die bereits verwendeten und zum Einsatz kommenden Technologien informieren, damit sie zumindest die Risiken kennen und vorbeugend einschreiten können. Wer sichergehen möchte, dass er nicht eines Tages für längere Zeit ohne Telekommunikation dasteht – insbesondere für Firmen ein Ding der Unmöglichkeit – sollte ein paar Euro mehr investieren und parallel zum bestehenden einen neuen Anschluss beantragen.

Für den Wechsel zwischen Anbietern fehlen an einigen Stellen technische und administrative Standards mit festen Zeitvorgaben für die einzelnen Vorgänge. Es könnte helfen, wenn hier die Bundesnetzagentur regulierend eingreift, damit das Wechseln nicht nur Geld, sondern auch Nerven spart. (un)

MANUEL SCHMITT

ist Geschäftsführer des Hosting-Unternehmens manitu.





Peer-to-Peer: Eigenes Suchportal mit Yacy einrichten

Wissen schürfen

Michael Christen

Trotz oder wegen der Monopolstellung, die Google mittlerweile im Suchmaschinenmarkt hat, existieren Projekte, die eine Alternative zu den Großen bieten wollen. Eines davon ist Yacy, das potenziell eine Vielzahl von verteilten Rechnern durchforsten kann.

Eine eigene Suchmaschine zu betreiben ist nicht nur für Anbieter großer Webportale mit Tausenden Seiten interessant, sondern auch als Spartensuche für Webseiten zu Spezialthemen. Wer in seinem CMS keine eingebaute Suchtechnik vorfindet oder aufgrund der Vielzahl der zu durchforstenden Sites einen separaten Crawler braucht, kann ein eigenes Portal mit Yacy (Yet another Cyberspace) aufbauen, das zudem im Peer-to-Peer-Verbund funktioniert und damit in Größenordnungen von Millionen Webseiten skalieren kann.

Yacy lag zum Jahreswechsel in der Version 0.56 vor und beinhaltet ein Peer-to-Peer-Protokoll, wobei die Organisation der Indexdaten so gestaltet ist, dass sie im Verbund der Yacy-Peers verteilt und leicht auffindbar sind. Es ist möglich, einen eigenen Such-Cluster mit Yacy-Peers zu definieren, sodass man eine skalierbare Suchmaschine aufbauen kann.

Jeder Yacy-Peer enthält einen Web-Crawler, einen Indizierer inklusive Parser für gängige Datenformate wie HTML, RSS, Word, RTF, PDF und weitere, eine eingebaute Datenbank-Engine und einen einfachen Application Server, der das P2P-, Administrations- und Such-Interface auf HTML-Basis beherbergt (siehe Abbildung 1).

Damit Webseiten in den Index gelangen können, muss ein Webcrawler zunächst deren Adressen erfassen. Nach der Bestimmung eines Startpunktes geschieht dies durch Laden von Webseiten, Scannen von Links in ihnen und wiederholtes Laden dieser Seiten. Doppelte Links filtert Yacy aus, außerdem sortiert das Tool unerwünschte Seiten gemäß Blacklists und gesperrten Pfaden entsprechend *robots.txt*-Anweisungen aus. Die Rekursion des Crawlers endet bei einer festgelegten Ladetiefe. Zudem beherrscht Yacy Balancing beim Zugriff auf Ziel-Domains, in dem es über alle bekannten Domains der URLs in der Ladeliste des Crawlers rotiert. Crawls können im P2P-Verbund kooperativ sein, das heißt auf Wunsch kann ein Crawl Teile seines Suchbaumes an andere Teilnehmer im Netz weiterleiten.

Zunächst erkennt der Indizierer sichtbare Texte in den geladenen Webseiten und Dateien, wozu verschiedene Parser zur Verfügung stehen. Betrachtet man Webseiten als URL/Wortmengen-Relation, besteht der Indizierprozess aus der Umkehrung dieser Relation zu einer Wort/URL-Mengen-Relation, das heißt einem Wort sind nach der Indizierung mehrerer Texte diverse URLs zugeordnet. Ein solcher Index heißt Reverse Word Index (RWI). Da jede Fundstelle einer URL im Wort-Index Ranking-Attribute beinhaltet, besteht ein Index daher konzeptionell aus vielen Tabellen, für jedes Wort eine. Jede dieser Tabellen hat als Hauptschlüssel eine Referenz (bei Yacy einen 12-stelligen Hash), der wiederum auf eine URL-Tabelle verweist und als Werte in der Indextabelle eine große Anzahl von Attributen zur Fundstelle hat, beispielsweise die Wortposition im Text und weitere Attribute zum Ranking.

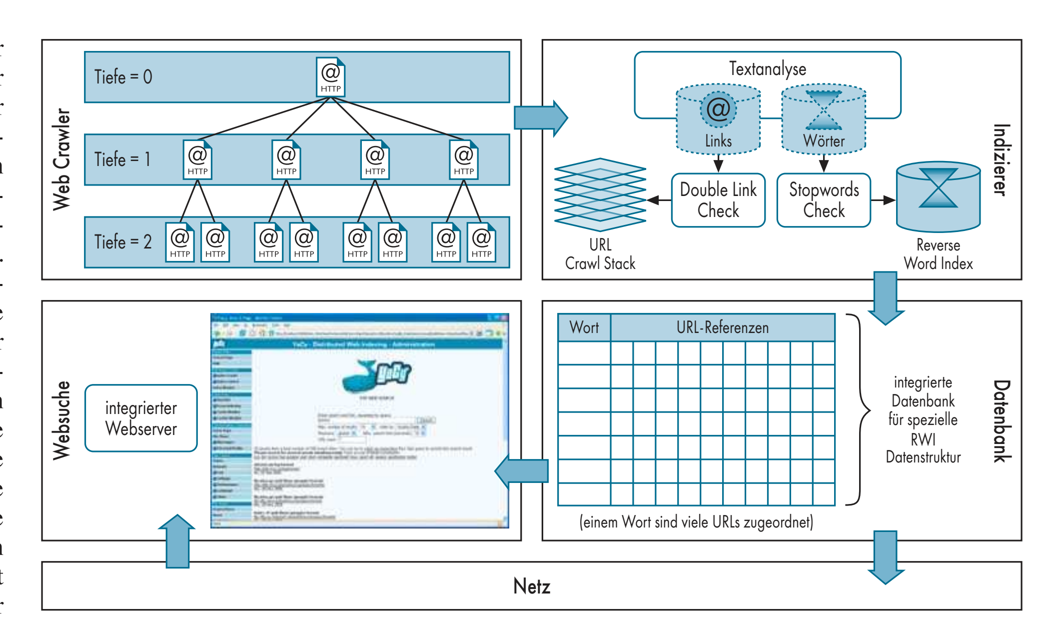
Spezialisierte Datenverwaltung

Die eingebaute Datenbank muss in der Lage sein, viele Tabellen für die Wort/URL-Mengenrelationen (eine für jedes bekannte Wort) zu speichern. Hierzu ist eine spezialisierte Datenstruktur besser geeignet als standardisierte SQL-Konstrukte. Yacy enthält eine auf RWI-Daten ausgerichtete Datenverwaltung, daher sind keine weiteren DB-Anbindungen notwendig.

Anfragen bestimmter Peers nach Suchergebnissen und ein anschließender Merge dieser Ergebnisse mit den eigenen Indexdaten stellen die Websuche dar. Dabei fragt die Yacy-

Instanz nicht alle Teilnehmer des Netzes ab, sondern nur diejenigen, die aufgrund ihrer Position im Netz das bestimmte Suchwort kennen sollten. Die zugehörige Datenstruktur nennt sich „Distributed Hash Table“ (DHT). Sie wird laufend dadurch aufgebaut, dass alle Peers eigene Indexdaten, die aufgrund der DHT-Regeln nicht zum eigenen Peer-Standort passen, an solche DHT-Targets (andere Peers) verschicken, sodass sie im Vorfeld einer Websuche schon dort vorliegen, wo sie bei der Suche zu erwarten sind. Damit Indexdaten selbst dann verfügbar sind, wenn der Teilnehmer offline ist oder Daten löscht, werden Indizes redundant verteilt. Das bewirkt eine gewisse Ausfallsicherheit für Suchergebnisse im Gesamtnetz.

Schließlich braucht eine Suchmaschine ein Portal, und die natürliche Umgebung für eine Websuche ist der Browser. Yacy beinhaltet dafür einen einfachen Application Server, der das Web-Interface des Suchportals und alle Seiten der Suchmaschine, ihrer Konfiguration und Monitoring-Optionen vorhält.



Anatomie der Peer-to-Peer-basierten Suchmaschine Yacy (Abb. 1).

Suchen im Cluster

Yacys Fähigkeit, eine Menge unabhängiger Suchmaschinen-Peers in einen Cluster zusammenzuschließen, nutzen Betreiber über ein öffentliches Netz, um eine alternative Suchmaschine zu beliebigen Themen zu betreiben. Die Suche über das eigene Portal in diesem Netz hat Vorteile gegenüber anderen Möglichkeiten:

– keine Zensur,
– Anonymität des Suchenden, da kein zentrales Logging von Anfragen existiert,
– transparentes Ranking und keine Beeinflussung der Suchergebnisse durch Marketing-Effekte.

Yacy ist Java-Software und Open Source. Die Installation ist einfach: auspacken und Startskript aufrufen; es startet unter anderem einen Webserver auf Port 8080. Unter der Webadresse *localhost:8080* kann man anschließend den Peer konfigurieren – hauptsächlich durch die Vergabe eines Passworts und eines Namens.

Jeder kann zum Yacy-Suchnetz Inhalte hinzufügen, alle Peer-Betreiber sind gleichberechtigt. Hinzufügen geschieht durch Starten eines Crawls, der kooperativ ablaufen kann, das heißt andere Peer-Betreiber bekommen Teile des Suchbaums zugewiesen. Unter Peer-Betreibern austauschbare Blacklists können unerwünschte Webseiten abweisen. Es existieren schon große Blacklists für Spam-Abwehr, außerdem solche zum Filtern von Online-Verkaufsplattformen.

Web Crawls selbst starten

Das Indizieren von Webseiten erfolgt über eine Seite des Web-Interface. Hier kann man verschiedene Attribute zum Lenken eines Web Crawls einstellen, beispielsweise seinen Startpunkt, die Tiefe und URL-Filter. Crawls können in der Breite über viele Domains erlaubt sein oder sich auf eine einzige Domain beschränken (Site Crawl). Außerdem gibt es Attribute für das erneute Indizieren von früher aufgenommenen Seiten. Weiterhin kann der Betreiber einen Crawl als kooperativ definieren – der Indizierer kann andere Peers um Hilfe bei der Bearbeitung des Crawl-Baumes bitten.

Da alle Funktionen in Yacy über ein Web-Interface erreichbar sind, kann man leicht mit *wget* alle Funktion skriptfähig machen. Im Falle des Crawl-Starts bietet sich das an, wenn eine Site regelmäßig erfasst werden soll, beispielsweise weil es eine Nachrichtenseite ist. Listing 1 zeigt einen solchen *wget*-Aufruf für die *iX*-News. Er könnte als Cron-Job täglich laufen.

Nach einem Start hat der Nutzer vielfältige Möglichkeiten, auf den entstehenden Index einzuwirken, den Prozess zu beobachten und über verschiedene Monitoring-Funktionen das Ergebnis des Crawls zu analysieren. Abbildung 2 zeigt die Menüstruktur von Yacys Web-Interfaces und als Monitoring-Beispielseite das Netzstrukturbild eines Crawls von *heise.de*. Dieses Bild kann man zu jeder Domain von erfassten Webseiten erstellen, und es könnte zur Analyse der Verlinkungsstruktur für jeden Betreiber einer Website dienen.

Ein eigenes Suchnetz

Statt bei der generellen Suche im öffentlichen Netz mitzumachen, kann der Anwender Yacy so konfigurieren, dass ein eigenes Suchnetz entsteht. Hiermit bietet sich Yacy auch als Alternative zu einer Appliance an, denn es kann mehrere Millionen Webseiten in einer einzigen Peer-Instanz

iX-TRACT

- Wenige Suchmaschinen wie Google bedeuten naturgemäß eine Abhängigkeit von deren Ergebnissen.
- Sich eine eigene Search Engine aufzubauen, kann selbst für Spartensites lohnenswert sein.
- Mit Yacy liegt frei erhältliche Software vor, mit der Website-Betreiber für sich oder im Peer-to-Peer-Verbund eine verteilte Suche skalierbar umsetzen kann.

Listing 1: Suche per *wget* vom Terminal aus

```
wget "http://admin:password@localhost:8080/WatchCrawler_p.html?crawlingDepth=2&crawling-
Filter=.*\.heise\.de/ix/.*&crawlingQ=on&localIndexing=on&crawlOrder=off&crawlingMode=
url&crawlingURL=http://www.heise.de/ix/&crawlingIfOlderCheck=on&crawlingIfOlderNumber=
1&crawlingIfOlderUnit=day&crawlingstart="
```

Listing 2: Netzdefinitionsdatei 'yacy.mynetdef'

```
Muss entsprechend eigener Bootstrap-Adresse angepasst werden
# Namenskürzel und Langbezeichnung des neuen Netzes
network.unit.name = mynet
network.unit.description = Mein erstes eigenes Yacy-Netz
# Domäne des Suchbereiches (local|global|any),
# bei 'global' werden nur öffentlich erreichbare Webseiten indiziert,
# bei 'local' nur Webseiten aus dem Intranet
network.unit.domain = any
# Attribute zur Redundanz, bei komplett kontrollierbaren
# hoch verfügbaren Teilnehmer-Peers empfiehlt sich '1'
network.unit.dhtredundancy.junior = 1
network.unit.dhtredundancy.senior = 1
# bootstrap-Adresse des Netzes, Speicherort der Seed-Lists die vom
# bootstrap-Peer (dem 'ersten' Peer) per seedlist-Upload generiert wird
network.unit.bootstrap.seedlist0 = http://www.meinedomain.de/yacy.myseedlist
# Update-Adresse für automatische Release-Updates
network.unit.update.location0 = http://yacy.net/yacy/Download.html
```

verwalten. Ist eine noch höhere Skalierbarkeit gewünscht, kann man mehrere Yacy-Peers in einem privaten Netz verschalten. Das Betreiben einer eigenen Suchmaschine bietet Privatpersonen, Unternehmen oder Bildungseinrichtungen Vorteile:

– Der Index bleibt auf selbstdefinierte Inhalte beschränkt, und Suchergebnisse können treffender sein als die eines öffentlichen Portals, das eventuell unerwünschte Inhalte beimischt.

– Suchen im eigenen Portal bleibt insofern anonym, als kein externes nachvollziehen kann, wonach gesucht wurde. Dies kann insbesondere für Unternehmen interessant sein, die auf Geheimhaltung ihrer Forschungsaktivitäten angewiesen sind.

– Wie aktuell Inhalte sein sollen, kann der Betreiber selbst bestimmen.

– Kommerzielle Such-Appliances sind recht teuer, und oft enthalten sie Beschränkungen bezüglich der Anzahl der erfassten Webseiten. Ein Yacy-Suchnetz ist dagegen in seiner Leistungsfähigkeit prinzipiell beliebig erweiterbar.

Für den Aufbau eines eigenen Suchnetzes muss man die voreingestellte Definition des öffentlichen durch eine eigene ersetzen. Dies ermöglicht die Erfassung von Intranet-Inhalten, deren Indizierung im öffentlichen Netz logischerweise ausgeschlossen ist. Die Netzdefinition muss bei allen Teilnehmern eines Netzes gleich sein. Über eine URL kann man die Definitionsdatei benennen (siehe unten). Der Aufbau eines neuen Netzes erfolgt in drei Schritten, zunächst durch Definition des ersten Peers und anschließend im Deploy der weiteren, die dem ersten zugeordnet sind:

– Erstellung der Netzdefinitionsdatei *yacy.mydef* entsprechend der Default-Datei *yacy.network.unit*. Listing 2 enthält eine Definition, mit der sich lokale und öffentliche Webadressen indizieren lassen,

– Upload dieser Datei zu einem Webserver, wo sie für alle nachfolgenden Peers des neuen Netzes erreichbar ist (www.meinedomain.de/yacy.mynetdef).

– Setzen eines Links auf diese URL für die Netzdefinition in *yacy.init*: *network.unit.definition = http://www.meinedomain.de/yacy.mynetdef*

Dieser Vorgang ist nur für die Erstinstallation notwendig, nach weiteren Updates der Peers jedoch nicht mehr. Nun kann es mit dem ersten Peer losgehen. Damit ein zweiter ihn finden kann, muss der erste seine eigene IP-Adresse publizieren; diese wird über den Menüpunkt *http://<addresse_erster_peer*

Suchmaschinen und Politik

Wer heute Informationen sucht, benutzt eine Suchmaschine. Die wiederum wählt aus, welche Informationen aus der unendlich erscheinenden Vielfalt sie anzeigt, und „entscheidet“ so darüber, was der Fragesteller findet (= weiß).

Noch sind die Nutzer von Suchmaschinen nicht auf Gedeih und Verderb den Big Search Brothers dieser Welt ausgeliefert (Google et al.), weil der Nutzer noch zwischen verschiedenen Angeboten auswählen kann. Aber es gibt davon immer weniger. Deswegen sind Initiativen wie Yacy wichtig. Denn nur wenn man Informationen von verschiedenen Anbietern mit unterschiedlichen Interessen und Sichtweisen einholen kann, besteht die Chance, dass eine einigermaßen objektive Sicht der Dinge zustande kommt.

Es gab im Jahr 2005 kurzzeitig einen Ansatz zum Gegensteuern in der sogenannten Schröder-Chirac-Initiative, die unter dem Namen Quaero bekannt wurde. In Europa sollte ein unabhängiges Gegengewicht zum US-amerikanischen Quasi-Monopol entstehen. Diesen Ansatz verfolgt Frankreich zwar noch; in Deutschland hat man sich jedoch entschlossen, mit dem Theseus genannten Quaero-Nachfolger die Zielrichtung zu verschieben: Theseus soll sich der Grundlagenforschung im Bereich des Semantic Web widmen, um damit das Internet der übernächsten Generation zu schaffen.

Rückzug ins Semantic Web

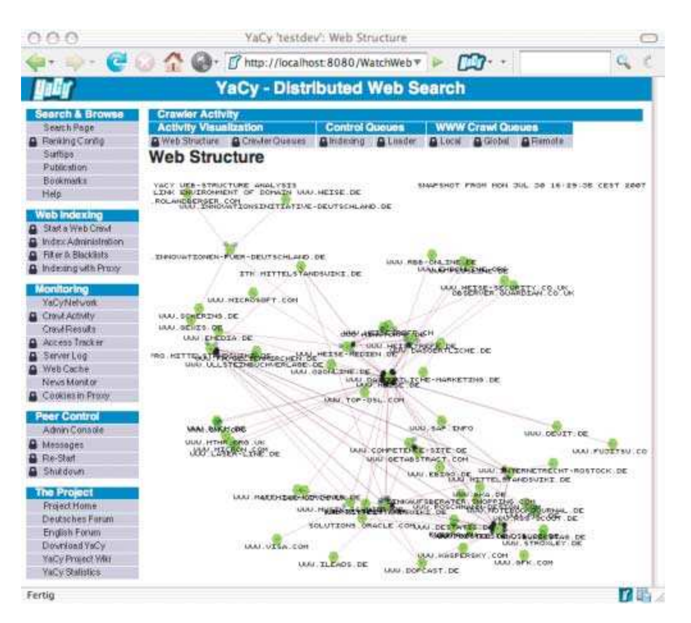
Was immer man über diese hehren Ziele und deren Machbarkeit oder Unmöglichkeit denkt – um eines kommt keine Informationsverarbeitung herum: die Bewältigung gewaltiger Datenmengen. Die dürften in zukünftigen Internet-Generationen mit Sicherheit nicht schrumpfen, sondern eher wachsen. Um die Informationen darin zu erschließen, betreibt der Suchmaschinen-Primus Google ein weltweites Netz von einigen Hunderttausend PCs mit optimierter Suchmaschinen-Software.

Und genau da liegt des Pudels Kern: Noch so viel Semantik hilft nicht, wenn es um die Verarbeitung und die Informationsextraktion aus riesigen Datenmengen geht. Letzteres ist das Basiswissen. Will man das Internet der übernächsten Generation ohne dieses Basiswissen schaffen, ist es so, als wollte man einen Porsche-Motor bauen, ohne zu wissen, wie eine Zündkerze funktioniert.

Mit dem Rückzug auf das Semantic Web muss man sich nun nicht mehr der Realität eines gigantischen und weiter wachsenden Internet stellen, sondern kann im Elfenbeinturm von Zukunftsvisionen träumen, ohne sich um die schnöde Praxis kümmern zu müssen. Man darf in diesem Turm in Ruhe Tischfussball spielen, aus der Bundesliga der Informationsgesellschaft hat Deutschland sich selber herausgekickt.

Da staatliche Organisationen versagen, bleiben diese Aufgaben für die Zivilgesellschaft. Projekte wie Yacy sind ein Teil davon, denn es schafft Vielfalt durch die unterschiedlichen Betreiber seiner Peers. Deren Netz schreckt nicht einmal vor großen Datenmengen zurück. Eine überschlägige Kalkulation, wie viele Peers man bräuchte, um auf dem Weltmarkt mitzuspielen, ergibt eine nicht utopische Zahl in der Größenordnung um 10 000. Selbst wenn es derzeit meist nur circa 100 Peers sind, die aktiv am Netz teilnehmen, sind das keine unrealistischen Perspektiven.

Wolfgang Sander-Beuermann



Yacys Menüstruktur und das Monitoring von *heise.de*, in der Mitte gerade so erkennbar, mit der Verlinkungsstruktur (Abb. 2)

Listing 3: Für Peers zu ändern in 'yacy.init'

```
# neue Netzdefinitionsdatei, muss angegeben werden
network.unit.definition = http://www.meinedomain.de/yacy.mynetdef
# optionale Attribute zu auto-update und default-Passwort
# (nur Beispiel, Passwort zum Web-Interface unbedingt individuell bestimmen)
update.process = auto
adminAccount = admin:myS3cr3tPa55w0rd
```

Listing 4: Einbettung einer Suchabfrage im Webformular

```
<!-- unter action die Adresse des eigenen Peers angeben -->
<form action="http://meinserver.de:8080/yacysearch.html"
     method="get" name="searchform" id="searchform">
<!-- das Suchfeld kann individuell in seiner Größe angepasst werden -->
<input name="search" type="text" size="16" maxlength="80" value="" />
<!-- display=2 lässt die Ergebnisseite ohne Yacy-Menüs drumherum erscheinen -->
<input type="hidden" name="display" value="2" />
<!-- count gibt die Anzahl der gewünschten Suchergebnisse an -->
<input type="hidden" name="count" value="10" />
<!-- resource selektiert p2p-Modus:
     local=nur vom eigenen Peer, global=Ergebnisse aus DHT -->
<input type="hidden" name="resource" value="local" />
<!-- time gibt die maximale Suchzeit in Sekunden an -->
<input type="hidden" name="time" value="3" />
<!-- urlmaskfilter ist eine regular expression (Java Stil) und selektiert damit
     einen bestimmten Teil des Index, kann benutzt werden um
     verschiedene Indexe in einer Yacy-Instanz zu verwalten.
     Beispiel: value=".*yacy.*" -- nur Ergebnisse mit yacy im domain namen -->
<input type="hidden" name="urlmaskfilter" value= ".*" />
<!-- prefermaskfilter ist eine regular expression, Suchergebnisse mit
     passender URL werden weiter nach vorne in der Ergebnisliste angezeigt -->
<input type="hidden" name="prefermaskfilter" value="" />
<!-- Suchknopf, löst Suche aus -->
<input type="submit" name="Enter" value="Suchen" />
</form>
```

>*/Settings_p.html?page=ServerAccess* im Feld *staticIP* zugewiesen. Der erste Peer muss als Principal operieren – in der Lage sein, eine Seedlist zu erzeugen, damit die nachfolgend gestarteten Peers den ersten finden können. Unter *http://<adresse_erster_peer>/Settings_p.html?page=seed* kann die Upload-Adresse für die zuvor in *yacy.mynetdef* eingetragene Seedlist stehen. Sie lautet

http://www.meinedomain.de/↵
yacy.myseedlist

Im zweiten Schritt wird eine spezielle Bootstrap-Release für alle teilnehmenden Peers des eigenen Netzes erstellt, damit neue Peers automatisch auf es zugreifen können. Ist ein neuer korrekt konfiguriert und ins Netz integriert, kann man ihn mit einer normalen, unveränderten Release aktualisieren, ohne dass die Netzzugehörigkeit verloren geht. Die Schritte zur Definition der Spezial-Release sind:

– Konfigurieren der Netzdefinition in *yacy.init*; siehe Listing 3.

– Ist *yacy.init* fertig konfiguriert, kann Yacy eine Bootstrap-Release für das eigene Netz einfach durch Einpacken des *yacy*-Verzeichnisses zur Verfügung stellen: *tar cfyacy_mynet.tar yacy*.

Für ein Massen-Deploy ist das Archiv *yacy_mynet.tar* auf die Rechner des Netzes zu verteilen und auszupacken.

Eigene Erweiterungen

Erweiterungen kann man auf zweierlei Weise ohne Veränderung des Programmcodes vornehmen: durch Nutzen der Servlets im eingebauten Web-Interface oder dessen Erweiterung um eigene Mini-Anwendungen. Letzteres ist nicht schwierig, würde aber den Rahmen des Artikels sprengen. Hilfe hierzu findet sich im Yacy-Wiki [b] oder im Forum [c].

Ein interessantes Interface-Servlet ist sicherlich die Ausgabe der Ergebnisse per XML. Es unterstützt den offenen Opensearch-Standard des Suchportals A9 [e]. Das Opensearch-Format ähnelt dem RSS-Format. Es ist leicht, diese Ausgabe zu prüfen: Nach einer Yacy-Suche ersetze man in der URL der Ergebnisseite *yacysearch.html* das *html* durch *rss*. *yacysearch.rss* bietet die Ergebnisse im Opensearch-Format an. Weiterhin existieren einige Servlets, die Statusinformationen über Yacy per XML liefern. Solche XML-Seiten finden sich unter *~yacy/htroot/xml*.

Um Yacy im eigenen Portal einzusetzen, muss nur ein Eingabefeld für Suchbegriffe eingebettet werden. Dieses Feld verweist auf eine Yacy-Instanz, die mehrere Webindizes verwalten kann, aus denen sie mit entsprechenden Tags die gewünschte Instanz auswählt. Ein Beispiel liefert die Installation der Suche für das Yacy-Wiki [b]. Hier kam im Template des MediaWiki ein neues Suchfeld zum Einsatz, das in Listing 4 zu sehen ist.

Suchergebnisse erscheinen in einem neuen Fenster als Ausgabe des Webservers. Damit sie in eigene Webseiten eingebettet werden können, kann dies auf einfache Weise in einem *iframe* dargestellt werden, oder etwas eleganter über einen Parser, der die Suchergebnis-Daten per RSS abfragt und innerhalb des eigenen Portals wieder darstellt.

Fazit

Yacy als Peer-to-Peer-Suchmaschine soll eine offene Alternative zu anderen Suchportalen bieten, jedoch eignet sich diese Technik mit wenigen Modifikationen durchaus zum Aufbau eines internen Suchportals. Im Stand-alone-Modus kann es als Alternative zu kommerziellen Search Appliances dienen. (hb)

MICHAEL CHRISTEN

ist freiberuflicher IT-Berater und Initiator des Yacy-Projekts.

Onlinequellen

[a]	Yacy-Homepage	yacy.net
[b]	Yacy-Wiki	wiki.yacy.de
[c]	Yacy-Forum	forum.yacy.de
[d]	deutschsprachige Dokumentation	yacy-websearch.net/wiki/index.php/De:Start
[e]	Opensearch	www.opensearch.org

Dynamische Programmierung unter .Net

.Net on Rails

Gerhard Völkl

Variablen, deren Typ erst zur Laufzeit festgelegt wird, oder Programme, die ihre eigenen Funktionen ändern, waren lange Zeit die Schreckgespenster des Software Engineering. Seit neue, dynamische Programmiersprachen wie Ruby oder Python auf den Plan traten, ist das alles so hip, dass selbst Microsoft zukünftig mit eigenen Varianten dieser Sprachen plus zusätzlichen Erweiterungen aufwarten will.

Mit Ruby on Rails [1] zeigten David Heinemeier Hansson und sein Team vor vier Jahren wie man ein Web-Framework für Datenbank-Applikationen so gestaltet, dass ein Entwickler möglichst schnell zu einem einsetzbaren Programm kommt. Aus wenigen Vorgaben über die verwendeten Tabellen generiert das Framework Rails eine erste lauffähige Version, bestehend aus HTML-Seiten und Code in der dynamischen Programmiersprache Ruby. Alles basiert auf den Grundprinzipien „Don't repeat yourself“ und „Convention over configuration“. Konvention bedeutet in diesem Fall, dass der Programmierer nicht alles explizit definieren muss, sondern Rails bestimmte Informationen nach festgelegten Regeln selbst ableitet. So steht der Name der Webseite in einem bestimmten Zusammenhang mit dem Namen der dort angezeigten Tabelle.

Die teils überschwänglichen Beifallsstürme, die Ruby on Rails bei manchen Webprogrammierern auslöste, muss man bis nach Redmond gehört haben. Auf der MIX Ende April 2007 erlaubte Microsoft einen ersten Blick auf die Technologien, die für die Nach-Visual-Studio-2008-Ära angedacht sind. Grundsatz ist auch hier: Weg vom statischen Ingenieursgehabe hin zur integrierenden Dynamik, die mehr Effizienz liefern soll.

Grundlage: DLR

Von der neu vorgestellten Technik beschäftigt sich dieser Artikel mit der Dynamic Language Runtime (DLR) – einer gemeinsame Basis für dynamische Programmiersprachen, der dynamischen Variante der Datenbank-API ADO.Net (Jasper) und den dynamischen ASP.Net-Steuerelementen.

Mit der ersten Version des .Net-Framework brachte Microsoft seine eigene virtuelle Maschine „Common Language Runtime“ (CLR) heraus. Sie ist die gemeinsame Basis unterschiedlicher Programmiersprachen wie C#, VB.Net und 100 weiterer [2]. Darunter sind auch dynamische Programmiersprachen (siehe Kasten), allen voran IronPython 1.0., eine Python-Version für .Net [3].

In diesem von Microsoft selbst geförderten Projekt mussten die Compiler-Bauer allerdings lernen, dass es schwierig ist, diese Art von Sprachen auf der Grundlage von CLR zu implementieren. Die Entwicklung eines guten Compilers, der performanten Code liefert, erfordert viel Erfahrung mit den .Net-Interna. Damit nicht jeder Sprachentwickler die gleichen Fehler noch einmal machen muss, stellt Microsoft für dynamische Sprachen die DLR als zusätzliche Komponente ober-



- Microsoft plant, für .Net dynamische Programmiersprachen, Datenbankzugriffe und Web Controls zu entwickeln, erste Vorabversionen sind verfügbar.
- Vorgabe der Softwaredesigner ist es, die dynamischen Bestandteile in die bestehende .Net-Philosophie zu integrieren und somit einen Austausch zwischen den „Welten“ zu gewährleisten.
- Zu diesem Zweck werden die dynamischen Bestandteile mit der Dynamic Language Runtime „vorbehandelt“. Microsoft hat so eine zusätzliche Compiler-Schicht in das .Net-Modell eingezogen.

halb von CLR zur Verfügung (siehe Abbildung 1).

In der aktuellen Alpha-Version gliedern sich die Funktionen der DLR in drei große Blöcke:

– ein gemeinsames dynamisches Typsystem,
– eine einfache API, mit der eine Programmiersprache in eine Applikation als Script-Sprache integriert werden kann (Hosting API),
– verschiedene Klassen, die den Compiler beim Erzeugen von schnellem dynamischen Code unterstützen (inklusive einer kompletten Konsolenoberfläche mit Debug-Möglichkeiten).

Auf Basis der DLR hat Microsoft zurzeit vier Programmiersprachen angekündigt: IronPython, IronRuby, Managed JavaScript und VBx, der mögliche Nachfolger von VB.Net 9.0. Der Quellcode der ersten beiden Sprachen und somit die Sourcen der DLR selbst stehen im Internet zur Verfügung. Die komplette DLR-Schicht ist im Namensraum *Microsoft.Scripting* abgebildet.

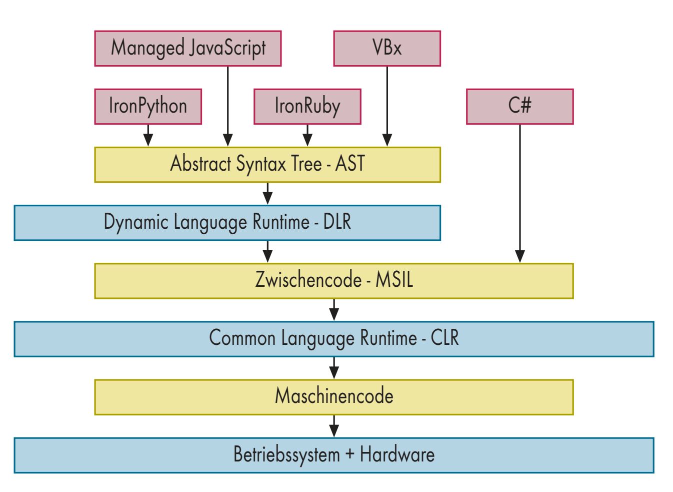
Die neuen Programmiersprachen können nur auf einen größeren Kreis von Entwicklern hoffen, wenn sie mit den vorhandenen .Net-Bibliotheken problemlos zusammenarbeiten. Eine Voraussetzung dafür ist ein gemeinsames Typsystem, mit dem die dynamischen Sprachen Klassen (Objekttypen) nicht nur gegenseitig nutzen, sondern auch Klassen der anderen .Net-Sprachen integrieren können. Die DLR soll den Zaubertrick vollführen, so verschiedene Typsysteme wie die statische Typisierung mit einfacher Vererbung von C# mit Pythons dynamischer Typisierung mit Mehrfachvererbung und Javascripts Typisierung mit Prototypen unter einen Hut zu bringen.

Jim Hugunin, der Softwarearchitekt von IronPython und der DLR, versucht es – wie er es in seinem Blog erläutert – mit einer grundsätzlichen Idee der Objektorientierung: Schicke einem Objekt eine Nachricht (Aufruf einer Methode) und lass es selbstständig antworten, ohne dich einzumischen. Diese gemeinsame objektorientierte Basis steht jeder Sprache zur Verfügung, unabhängig davon, welches Typsystem sie hat. Die Anzahl dieser Nachrichten, auf die jedes Objekt antworten können muss, ist in der momentanen Version von DLR relativ klein.

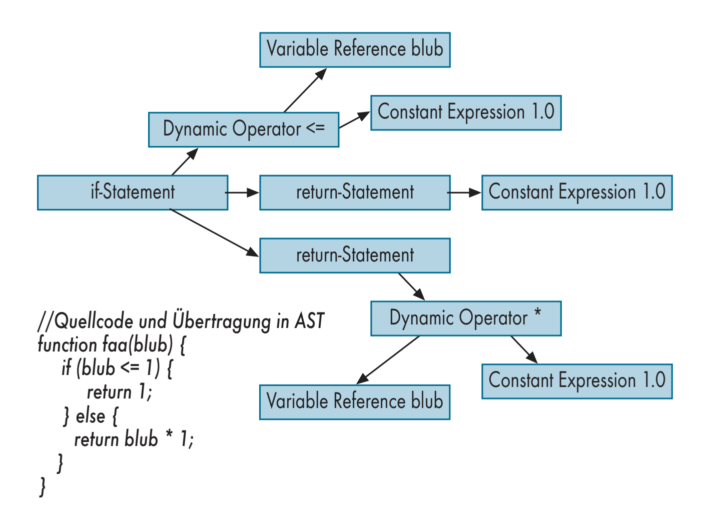
Diese Standardnachrichten werden auch als „Actions“ bezeichnet und sind konsequenterweise im Namensraum *Microsoft.Scripting.Action* untergebracht. Die DLR muss dafür sorgen, dass jeder Typ diese Standardmethoden besitzt. Bei den Objekten der neuen Programmiersprachen ist das relativ einfach, da hier per Definition alle Objekte das Interface *Microsoft.Scripting.IDynamicObject* implementieren müssen, was genau den Standardmethoden entspricht. Kritisch wird das Ganze bei Objekten, die von anderen Programmiersprachen stammen, wie bei allen Standard-.Net-APIs, da die DLR hier selbst einen Mechanismus realisieren muss, der diese Funktionen zur Verfügung stellt. Nur wenn Jim Hugunin und seine Mitstreiter dies so bewerkstelligen können, dass alles performant und ohne Kompatibilitätsprobleme läuft, haben neue Sprachen die Chance, einen größeren Nutzerkreis zu gewinnen.

Ein weiterer Vorteil, den ein Compiler-Bauer durch die DLR hat, ist die Vereinfachung der Übersetzung des Quellcodes in den IL-Zwischencode (Intermediate Language), mit dem die CLR arbeitet. Der Compiler braucht den Source-Text lediglich in eine Baumstruktur zu übersetzen, als Abstract Syntax Trees (AST) bezeichnet, die DLR übernimmt dann die Übertragung in Zwischencode, inklusive Optimierung (siehe Abbildung 2).

Diese Vorgehensweise ist nicht neu, es gibt sie schon



Für dynamische Sprachen ist die Dynamic Language Runtime als zusätzliche Schicht über die Common Language Runtime eingezogen (Abb. 1).



Der erzeugte Abstract Syntax Tree ist die Vereinheitlichung aller dynamischen Sprachen unter .Net und wird von der Dynamic Language Runtime in Microsoft Intermediate Language Code übersetzt (Abb. 2).

seit der Entwicklung der Programmiersprache Lisp in den Fünfzigerjahren des letzten Jahrtausends. In Lisp ist die AST-Struktur unter dem Namen SExpr (Symbolic Expression) bekannt. Unter dem Namen „Expression Trees“ hielt sie durch Linq [4] Einzug in C# 3.0 und VB.Net 9.0.

An dieser Stelle schließt sich der Kreis, denn die DLR übernahm die Klassen des Expression Tree von C# 3.0 und fügte zusätzliche Knoten für dynamische Operatoren, Variablen und andere Erweiterungen hinzu. Durch die Entwicklung von DLR zusammen mit den vier neuen dynamischen Programmiersprachen, stehen die Chancen nicht schlecht, dass hier praxisnahe Komponenten im Entstehen begriffen sind, die das Optimum aus der CLR herausholen.

Dynamisches ADO.Net

Unter dem Codenamen „Jasper“ arbeitet Microsoft an einem Nachfolger von ADO .Net 3.0, der Bestandteil von Visual Studio 2008 ist. Das primäre Ziel dieser neuen Datenbank-API ist die Unterstützung einer möglichst interaktiven und schnellen Anwendungsentwicklung. Im angestrebten Idealfall braucht der Programmierer Jasper lediglich

mitzuteilen, mit welcher Datenbank er arbeiten möchte und kann sofort loslegen, ohne groß zu konfigurieren oder zu warten, bis eine Menge Code generiert wurde, wie bei *TableAdapter* von ADO.Net. Jasper arbeitet mit allen aktuellen Microsoft-Frameworks (ASP.Net, WinForms, WPF) und den gängigen Datenbanken zusammen. Zwei Funktionsbereiche sind von größerer Bedeutung: erstens der einfache Zugriff auf eine Datenbank, mit dem Entwickler ohne viel Aufwand Informationen abfragen oder aktualisieren können, und zweitens eine möglichst automatisierte Verbindung zwischen den Steuerelementen der Benutzeroberfläche und der Datenbank. Der zentrale Dreh- und Angelpunkt der API ist die Klasse *DynamicContext*. Sie kümmert sich um die Datenbankverbindung und kapselt den aktuellen Zustand der Daten.

```
Dim connectionString As String ⏎
        ="...;Default EDM=True;"
Dim context as DynamicContext = ⏎
DynamicContext.CreateDynamic ⏎
        Context(connectionString)
```

Der *ConnectionString*, den die *DynamicContext*-Klasse beim Erzeugen erhält, unterscheidet sich nur durch die letzte Klausel von einem für ADO.Net 3.0. Diese zusätzliche Definition weist Jasper an, die Klassen für die Verbindung zwischen relationaler Datenbank und objektorientierter Programmiersprache selbst zu erzeugen.

Intern arbeitet die API mit dem *Entity*-Framework von ADO.Net 3.0, der neuen objektrelationalen Datenbankschnittstelle von Microsoft. Dieses Framework erwartet normalerweise, dass der Programmierer die Datenklassen von Hand kodiert oder alternativ mit einem Tool in der Entwicklungsumgebung generiert. Jasper dagegen liest selbst die Schemainformationen aus der Datenbank und erzeugt zur Laufzeit für jede Tabelle eine Datenklasse und für jede Spalte eine Property. Die Beziehungen von Primär- und Fremdschlüssel geben Aufschluss, für welche Spalten Methoden zur Navigation zwischen den Klassen notwendig sind.

Wenn sich die Datenbank häufig ändert, ist die Generierung zur Laufzeit sehr vorteilhaft, denn wenn der Entwickler bei einer klassischen Datenbank-API vergaß, die Verbindungsklassen nach dem Hinzufügen eines neuen Feldes zu aktualisieren, kam es zu Laufzeitfehlern, auch wenn das neue Feld gar nicht angesprochen wurde.

Voraussetzung für das Erzeugen der Klassen durch die API sind Programmiersprachen, die *Late*-Bindung unterstützen, wie die aktuelle Version von VB.Net, oder ein dynamisches Typsystem haben, wie IronPython und die anderen angekündigten dynamischen Programmiersprachen. Es zeigt sich hier, dass diese flexibleren Sprachen die Voraussetzung sind, um das Entwicklerleben zu vereinfachen.

Die automatische Ableitung der Klassen durch Jasper funktioniert nur, wenn die Datenbank „passend" aufgebaut ist. Ist dies nicht der Fall, hat die neue API spezielle Funktionen, mit denen der Programmierer nacharbeiten kann:

– *Naming service customization*: Der Entwickler kann, muss aber nicht festlegen, wie

Dynamische Programmiersprache

Für den Begriff „dynamische Programmiersprachen" gibt es im Netz die unterschiedlichsten Definitionen. Die meisten Quellen sind sich einig, dass Ruby, Python oder Basic dazugehören. Auch der Begriff Script-Sprachen wird oft im selben Atemzug genannt. Was aber nun eine dynamische Programmiersprache von anderen genau unterscheidet, ist nicht exakt festzumachen. Die einzige Grundaussage, auf die sich alle einigen können, ist, dass dies Sprachen sind, die bestimmte Dinge erst zur Laufzeit tun, wie Variablen binden oder Ähnliches, was bei anderen schon beim Kompilieren passiert.

Um diese Sprachen etwas genauer eingrenzen zu können, hat Ed Johnson auf seiner Website drei Eigenschaften herausgearbeitet, die die meisten besitzen; manche aber auch wieder nicht:

– dynamische Typisierung,

– Ändern oder Erzeugen von Programmbestandteilen,

– interpretierend – kein Compiler.

Typisierung: Durch die Typisierung ordnet eine Programmiersprache ihre Bestandteile in bestimmte Gruppen ein. Variablen sind einem bestimmten Typ zugeordnet. Objekte gehören zu einer Klasse. Der Sinn dieses ganzen Aufwands liegt ganz klar in der Vermeidung von Fehlern. Dass ein Aufaddieren von Integerzahlen mit Zeichenkette nicht gut gehen kann, wird erkannt, bevor der Speicher überläuft.

Bei der Einordnung des Typsystems einer Programmiersprache gibt es grundsätzlich drei Kriterien:

– Stärke der Typisierung (stark – schwach),

– Dynamik der Typisierung (dynamisch – statisch),

– Explizität der Typisierung (explizit – implizit).

Eine Programmiersprache ist stark typisierend, wenn sie auf die Unterscheidung der Typen achtet und diese kontrolliert. Im klassischen C kann ein Programmierer mit einem Zeiger als Parameter jeden beliebigen Datentyp übergeben oder zur Laufzeiten mit Casting jeden Typ in einen anderen umdeklarieren. Ein klassischer C-Compiler prüft nicht, ob das sinnvoll ist, was früher häufig zu den Speicherüberläufen führte. C ist damit eine schwach typisierende Sprache, was eher den dynamischen Sprachen wie Python nachgesagt wird. Python hingegen prüft sehr stark, ob die Typen zur Laufzeit zusammenpassen. Ein entscheidendes Merkmal für ein dynamisches Typsystem ist, dass die Typen zur Laufzeit festgelegt werden können und nicht nur bei der Kompilierung, wie es bei statischen Systemen üblich ist.

Was eigentlich nichts mit einem dynamischen Typsystem zu tun hat, ist die Frage, ob eine explizite oder eine implizite Typdefinition möglich ist. Bei der expliziten Vorgehensweise muss der Programmierer, bevor er einer Variablen einen Wert zuweisen kann, diese erst deklarieren, bei der impliziten definiert die erste Zuweisung einer Variablen den Typ. Übrigens: Dieses Feature gibt es jetzt auch in den mit Visual Studio 2008 ausgelieferten Versionen von C# und VB.Net für lokale Variablen.

Programmänderung zur Laufzeit: Das sich ein Programm noch zur Laufzeit durch den Entwickler oder womöglich durch das Programm selbst ändert, klingt im ersten Moment etwas exotisch. Doch es gibt dafür einige sinnvolle Anwendungen. Kann erst das Laufzeitsystem feststellen, welche externe Schnittstelle eine bestimmte Klasse benötigt, ist es keine Magie, die Schnittstellen-Klasse erst dann zu erzeugen.

Ein ähnliches Thema sind SQL-Statements, die eine Programmroutine erst bei der Anwendung vervollständigt. In vielen Programmiersprachen kann dies der Entwickler nur mit Zeichenketten bewältigen, da das Statement nicht zur Laufzeit in Objekte und Methoden umgewandelt werden kann.

Interpreter: Das Gegensatzpaar Compiler vs. Interpreter gibt es in der Informatik immer seltener. Der klassische Compiler, der alles zur Laufzeit in festen Maschinencode übersetzt, ist eine aussterbende Spezies. Moderne Programmiersprachen, ob Java, C# oder Python, arbeiten mit Zwischencode, der zur Laufzeit von einem Just-in-time-Compiler übersetzt oder gleich von einer virtuellen Maschine – einem Interpreter – abgearbeitet wird.

Tabellen- und Spaltennamen in Klassen- und Eigenschaftsnamen umgesetzt werden. Dies ist sinnvoll, wenn die Datenbank keine sprechenden Tabellennamen, wie etwa „dta_fpl_customer_1“, verwendet.
– *Data model customization*: Wenn die Datenbank keine einfache Struktur hat, kann man ein eigenes *Entity Data Model* definieren.

Um eine Verbindung zwischen der Datenbank und Steuerelementen in einem Dialog herzustellen, reicht der folgende Befehl:

```
Dim binder As New AutoBinder⁊
    (context, myForm)
```

Damit das ohne weiteres Zutun funktioniert, setzt die Klasse *AutoBinder* einige Konventionen voraus. Die Form muss ein *BindingSource*-Objekt haben, dessen Namen dem der Datenbanktabelle entspricht, die angezeigt oder bearbeitet werden soll. Analog geht Jasper auch bei den Steuerelementen vor. Ein Oberflächen-Steuerelement wird immer an die Eigenschaft der Datenklassen mit demselben Namen gebunden. Hält sich ein Entwickler an diese Vorgaben, bekommt er ohne zusätzliche Tipparbeit eine Zuordnung zwischen Steuerelementen und Datenbank.

Da die aktuelle Version von Jasper nur ein fortgeschrittener Prototyp ist, ist es noch zu früh, ein Urteil über die Performance zu fällen. Wenn momentan das *DynamicContex*-Objekt die Verbindungsklassen generiert, dauert das schon ein oder zwei Sekunden. Und das passiert natürlich jedes Mal, wenn die Applikation startet. Ein weiterer offener Punkt ist das Fehlen einer Unterstützung von IntelliSense. Das komfortable Ergänzen der Namen von Datenklassen zum Beispiel, scheitert in der Entwicklungsumgebung daran, dass zu diesem Zeitpunkt diese Klassen noch nicht vorhanden sind. Vom Jasper-Entwicklungsteam war aber zu hören, dass hier an einer Lösung gearbeitet wird.

Dynamisches ASP.Net

Dynamische Data Controls (DDC) für ASP.Net gehen noch einen Schritt weiter als Jasper. Sie stellen nicht nur die Verbindung zwischen Oberfläche und Datenbank her, sondern erzeugen die gesamte Benutzerschnittstelle gleich mit. Diese neuen Server Controls lesen zur Laufzeit die Informationen über den Aufbau der Tabellen aus der Datenbank und erzeugen daraus möglichst selbstständig komplette Verarbeitungsdialoge.

Der Startpunkt für eine neue Webanwendung mit diesen Steuerelementen ist die Projektvorlage „Dynamic Data Web Site“. Die Designer der Controls gehen davon aus, dass in den meisten Fällen eine Datenbanktabelle auf genau einer Webseite dargestellt wird. Für eine Webseite für die *Table Customers* der Microsoft-Beispieldatenbank Northwind muss ein Entwickler lediglich ein neue Seite mit dem Template „Dynamic Data Web Form“ und den Namen *Customers.aspx* erzeugen. Das Ergebnis (siehe Abbildung 3) ist ein Formular, das die komplette Funktionalität zum Erzeugen, Bearbeiten, Löschen und Anzeigen der Kunden enthält. Die generierte ASP.Net-Seite (siehe Listing) enthält keinerlei Information über die auszugebenden Daten.

Die benötigten Informationen verschafft sich das einzige Steuerelement der Seite *DynamicAutoData* selbstständig. Als Erstes nimmt es Verbindung zur Datenbank auf, deren *Connection*-String es in der *web.config*-Datei findet. Gibt es mehrere, muss der Entwickler im Abschnitt *<dynamicDataControls>* von *web.config* angeben, welche Datenbank er gern hätte. Welche Tabelle angezeigt werden soll, leitet das Steuerelement aus dem ASP.Net-Seitennamen ab. Es gilt die Konvention: Der Name der Seite muss dem der gewünschten Tabelle entsprechen. Eine möglichst sinnvolle Darstellung in Tabellenform übernimmt intern das Steuerelement *DynamicList*, das wiederum zur eigentlichen Ausgabe das Standard-ASP.Net-Steuerelement *GridView* verwendet. Dies hat den Vorteil, dass Microsoft nichts extra entwickelt musste und alle Features fürs Seitendesign, wie *Skins* oder *Themes*, automatisch unterstützt werden.

DynamicList identifiziert die Spalten, für die Fremdschlüssel definiert sind, und erzeugt dafür *DropDownlists* mit passenden Werten. Momentan verwendet es die erste Nicht-Schlüsselspalte der Tabelle als Anzeigewert, auf die der Fremdschlüssel verweist. Dieses Arbeiten mit Konventionen kann natürlich schiefgehen. Das Beispiel dafür ist die Customer-Tabelle selbst. Verweist eine andere Tabelle auf diese, ist die erste Nicht-Schlüsselspalte von Customer der Vorname des Kunden. Damit kann ein Anwender wenig anfangen, besser wäre die dritte Spalte, in der der Nachname steht.

Da das Ableiten des Tabellennamens aus dem Seitennamen nur eine Seite pro Tabelle möglich macht, gibt es noch eine weitere Konvention, die den Tabellennamen aus

Namensräume der Dynamic Language Runtime

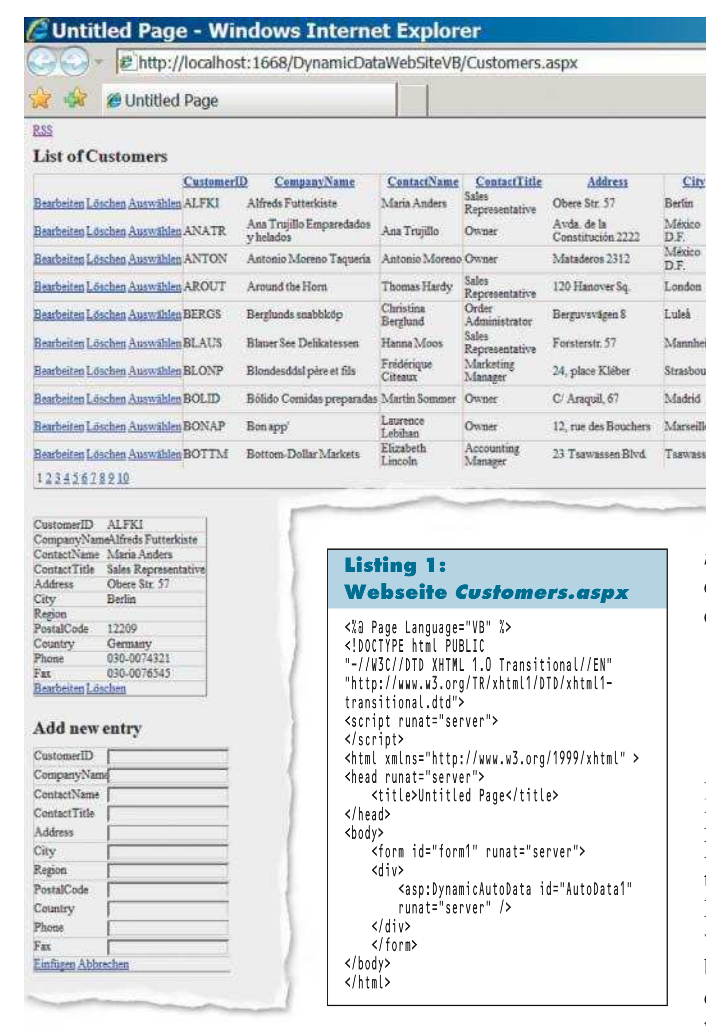
Namensraum	Beschreibung
Microsoft.Scripting	Basisklassen und Klassen, die Grundfunktionen zur Verfügung stellen
Microsoft.Scripting.Actions	alles für die Kommunikation mit dynamischen Objekten
Microsoft.Scripting.Ast	Knoten des Abstract Syntax Tree
Microsoft.Scripting.Generation	Klassen für Codegenerierung
Microsoft.Scripting.Hosting	zum Einbinden in andere Programme wie Silverlight und Browser
Microsoft.Scripting.Math	Zahlentypen, die bisher nicht unterstützt wurden, wie BigInteger oder Complex64
Microsoft.Scripting.Shell	komplette Konsole
Microsoft.Scripting.Types	Typen, die zur Erweiterung von bestehenden Typen verwendet werden

Methoden eines Objektes in der DLR

Nachricht (Methode)	Erläuterung
[Get / Set / Delete]Member(name, case-sensitivity)	liest, setzt oder löscht eine bestimmte, benannte Member eines Objektes; eine Member kann in diesem Fall ein Attribut, eine Eigenschaft oder eine Methode sein.
Call/CreateInstance(argument modifiers)	Standardaufruf oder „neu“-Aufruf für ein Objekt mit Argumenten
SimpleOperation(OperationKind enumeration)	beinhaltet alle einfachen gemeinsamen Operationen, wie *add* oder *subtract*.
Convert(Type)	konvertiert das Objekt, falls möglich, in den angegebenen, statischen Typ.

Übersicht der Dynamic Data Controls

Steuerelement	Funktion
DynamicAutoData	stellt eine Tabelle selbstständig in einem *GridView*-Steuerelement zusammen mit weiteren Steuerelementen für Eingabe und Filtern der Daten dar.
DynamicList	zeigt die aktuelle Tabelle in einem passenden *GridView*-Steuerelement.
DynamicDetails	Detaildarstellung einer Zeile der aktuellen Tabelle
DynamicFilter	erlaubt komfortables Filtern von Tabellenzeilen.
DynamicInsert	Anwender kann neue Zeile einfügen
DynamicNavigator	gibt eine Liste aller Tabellen und Ansichten aus, auf die in der Anwendung mit Dynamic Data Controls zugegriffen werden kann.
DynamicRssLink	stellt die Daten der aktuellen Seite als RSS-Feed zur Verfügung.



Listing 1: Webseite *Customers.aspx*

```
<%@ Page Language="VB" %>
<!DOCTYPE html PUBLIC
"-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-
transitional.dtd">
<script runat="server">
</script>
<html xmlns="http://www.w3.org/1999/xhtml" >
<head runat="server">
    <title>Untitled Page</title>
</head>
<body>
    <form id="form1" runat="server">
    <div>
        <asp:DynamicAutoData id="AutoData1"
        runat="server" />
    </div>
    </form>
</body>
</html>
```

Die Seite für die Ausgabe der Dateien und die Möglichkeit der Änderung ist ohne eine Zeile handgeschriebenen Code entstanden (Abb. 3).

dem Verzeichnisnamen abgeleitet. Soll etwa eine Anwendung drei Formulare für Customer haben, reicht es aus, dass der Entwickler drei Dateien erzeugt (beispielsweise: *~/Customers/list.aspx*, *~/Customers/details.aspx* und *~/Customers/undnocheineSeite.aspx*).

Die erste Seite wird aufgrund ihres Namens „list.aspx“ eine Darstellung der Tabelle in Listenform enthalten und nach der gleichen Logik die zweite Seite eine Detaildarstellung. Der Entwickler kann das Verhalten der neuen Steuerelemente wie bei allen anderen ASP-Steuerelementen über ihre Attribute anpassen; darüber hinaus kann er Funktionen überschreiben. Die nachfolgende Funktion definiert, welche Spalten die Tabelle anzeigen soll:

```
Overrides Function GetColumns() ⁊
                    AsIEnumerable
Return New Object() ⁊
    {"CustomerID", "CompanyName"}
End Function
```

Das *DynamicAutoData*-Steuerelement generiert zwar alles selbst, aber dadurch hat man als Entwickler im Detail oft zu wenige Eingriffsmöglichkeiten. In der Praxis wird es häufig sinnvoller sein, ein *DynamicList*-Steuerelement oder eines der anderen selbst auf einer Seite zu platzieren.

Fazit: Rote oder blaue Pille

In einer Schlüsselszene des Films „Matrix“ muss sich der Held entscheiden, ob er die rote oder die blaue Pille nimmt. Nimmt er die blaue, kann er weiter in einer Traumwelt leben und bekommt nichts von der Realität mit. Bei der roten muss er sich den wirklich existierenden Problemen stellen. Nach drei Versionen .Net ist auch Microsoft mit seinen Entwicklungswerkzeugen bei dieser Entscheidung angelangt. Was die Redmonder im Bereich Datenbank-Entwicklung mit ADO.Net 1.0 und 2.0 zusammen mit *DataSets, TableAdapter* und Ähnlichem geboten haben, war zwar objektorientiert, aber für den Einsatz im kommerziellen Umfeld zu umständlich. Eine hohe Produktivität war nur durch spezielle Frameworks, Generatoren oder zusätzliche Tools möglich.

Ein Grund für die relativ schnelle Verbreitung von Ruby on Rails ist die Fokussierung auf die Nische der Web-Datenbank-Applikationen. Dieser schmale Streifen aus dem Spektrum aller möglichen Applikationen, in dem wahrscheinlich ein Großteil der kommerziellen Entwickler tätig ist, wird von Rails effizient abgedeckt. Setzt Microsoft in Zukunft zur Aufholjagd mit produktiveren APIs, Oberflächen und wenn es sein muss, auch mit dynamischen Programmiersprachen an? (WM)

GERHARD VÖLKL

ist bei einem öffentlichen Transportunternehmen für Software zuständig. Außerdem arbeitet er als Fachautor für Data Mining und Data Warehouse.

Literatur

[1] Dave Thomas, David Heinemeier Hansson; Agile Webentwicklung mit Rails; Hanser Verlag, 2005

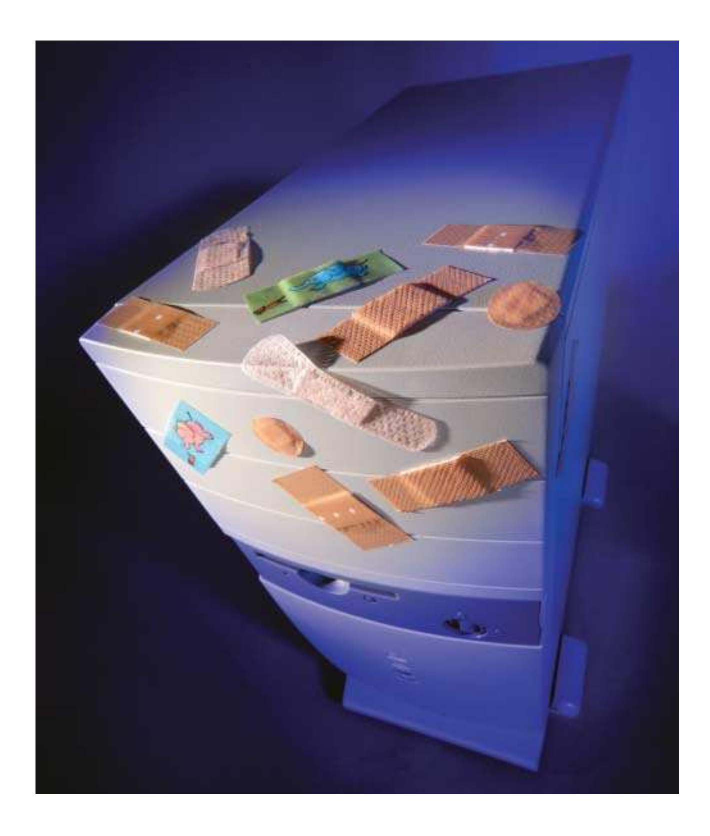
[2] Holger Schwichtenberg; Babylonische Vielfalt; Marktübersicht: .Net-Programmiersprachen; *iX* 10/2007, S. 102

[3] Thomas Kaufmann; Schlangengrube; Python-Implementierung für .Net; *iX* 2/05, S. 67

[4] Gerhard Völkl; Eingeflochten; .Net-Spracherweiterung: „Language Integrated Query“; *iX* 2/07, S. 110

Onlinequellen

Jim Hugunin; Zen of the DLR – Platforms, Balance and Working Code	www.iunknown.com/files/zen_of_the_dlr.pdf
Jim Hugunin's Thinking Dynamic: Dynamic Languages on .Net – IronPython and Beyond	blogs.msdn.com/hugunin/
Blog von John Lam, Software Architekt von IronRuby	www.iunknown.com/ Links
Ed Johnson: Invasion Of The Dynamic Language Weenies	www.hacknot.info/hacknot/action/showEntry?eid=93
mehr über Ruby On Rails	www.rubyonrails.org/
alles über IronPython	www.codeplex.com/IronPython
alles über IronRuby	www.ironruby.net/



Change-Management und Informationssicherheit

Up to date

Ronny Frankenstein, Wilhelm Dolle

Nahezu täglich sind an Unternehmensrechnern und -systemen Änderungen vorzunehmen – seien es Updates, Sicherheits-Patches oder gar Hardware- oder Betriebssystemwechsel. Definierte Prozesse beim sogenannten Change-Management sollen helfen, den Überblick zu behalten und alle Systeme gefahrlos auf den gewünschten Stand zu bringen.

Kein Unternehmen kann heutzutage auf ein geregeltes Change-Management verzichten. Das liegt unter anderem an der wachsenden IT-Abhängigkeit der Geschäftsprozesse und dem Versuch, diese stets zeitnah an geänderte wirtschaftliche Rahmenbedingungen anzupassen. Bei der Planung und Durchführung der notwendigen Änderungen darf die Sicherheit nicht auf der Strecke bleiben und muss im Change-Management-Prozess berücksichtigt werden.

Nahezu jeder IT-Anwender bekam die Auswirkungen eines fehlenden oder mangelhaften Change-Management schon einmal zu spüren. Typische Beispiele dafür sind:
– unzureichend getestete Änderungen werden „ausgerollt“ und sorgen für den Ausfall eines Dienstes,
– automatische Update-Funktionen von Software installieren Komponenten nach, die der Administrator gar nicht auf seinem System haben will,
– ohne eine kontrollierte Softwareverteilung werden viel zu viele Lizenzen einer Software installiert,
– oder es verbreiten sich Würmer über das Internet, die Sicherheitslücken ausnutzen, für die schon seit geraumer Zeit Sicherheits-Patches existieren, die aber niemand auf den Systemen installiert hat.

Zudem werden in Unternehmen häufig große Anschaffungen getätigt oder Projekte durchgeführt, ohne jemanden aus der IT-Sicherheitsabteilung zu informieren und einen fachlichen Rat zu den geplanten Änderungen oder Neuerungen einzuholen. Die genannten Szenarien lassen sich dadurch entschärfen, dass man ein Change-Management unter Einbeziehung der IT-Sicherheitsverantwortlichen einführt.

Um einen geeigneten Change-Management-Prozess für ein Unternehmen zu entwerfen, sollte man sich zunächst überlegen, welche Gruppen Änderungsanforderungen, sogenannte Requests for Changes (RfCs), initiieren. Eine naheliegende Quelle solcher Anforderungen ist das Sicherheitsmanagement eines Unternehmens selbst – etwa, wenn Informationen über neue Schwachstellen und entsprechende Sicherheits-Patches veröffentlicht werden, oder beim Aufarbeiten eines Sicherheitsvorfalls.

Neben Sicherheitsaspekten gibt es eine ganze Reihe weiterer Gründe für Änderungen an der IT-Infrastruktur. Die IT-Abteilung erhält interne Anforderungen von den für die Geschäftsprozesse verantwortlichen Fachabteilungen, die die Beseitigung von Störungen oder die Anpassung der IT an geänderte Verfahren fordern. Folglich hat sich das Change-Management an den Bedürfnissen der Geschäftsprozesse einer Firma auszurichten.

Eine weitere große Quelle von RfCs ist die IT-Abteilung, die typischerweise Störungen behebt, außerdem unkontrollierte Softwarestände verhindern und Client- und Lizenzmanagement durchführen soll.

Änderungen nicht ungefährlich

Auch wenn Änderungen im Rahmen des Change-Management häufig durchgeführt werden, um Störungen zu beseitigen, sind sie selbst eine potenzielle Bedrohung für die Sicherheit und die Geschäftsprozesse. Mit organisatorischen und technischen Maßnahmen gilt es daher, eine Verletzung der Sicherheitsziele Vertraulichkeit, Integrität, Verfügbarkeit und Verbindlichkeit aufgrund ungeeigneter Patches, Updates und Änderungen zu verhindern. Dazu sollte man sich zunächst die Gefahren genauer ansehen – einige typische seien hier genannt.

Die Hintergründe der Bedrohungen durch das Change-Management selbst sind vielfältig. Einige, etwa die unvollständige Bestandsaufnahme der Zielressourcen, die mangelhafte Berücksichtigung mobiler Systeme und die ungenügende Bereitstellung technischer, personeller und finanzieller Ressourcen, resultieren bereits aus einer unprofessionellen Einführung des Change-Management-Prozesses.

Andere wie fehlende Verantwortlichkeiten und Kommunikation zu anderen Beteiligten im Unternehmen, eine mangelhafte oder nicht durchgeführte Rollout-Planung sowie ein schlechtes

Notfallvorsorgekonzept und ungenügende Tests der Änderungen seitens der Fachabteilung sind oft festzustellen, wenn Change-Management ausschließlich als rein technisches Thema angesehen und der IT-Abteilung zugewiesen wird.

Durch seine zentrale Bedeutung für ein Unternehmen – insbesondere, wenn man Change-Management softwareunterstützt durchführt – sind einige weitere spezifische Gefährdungen zu berücksichtigen. Etwa der Missbrauch von Systemen oder Softwareänderungen, falls niemand deren Integrität sichergestellt hat.

Weg ohne Wiederkehr

In der Vergangenheit gab es gelegentlich Berichte über Update-Pakete, die Anwendern von Angreifern mit Softwareverteilungsmechanismen untergeschoben wurden. Es bestehen außerdem zusätzliche Gefahren, wenn man nach einer fehlgeschlagenen Änderung nicht wieder in den Ausgangszustand zurückkehren kann.

Gerade in der Kombination mit der automatischen Verteilung von Patches, Updates und Änderungen auf eine große Anzahl von Anwendungen und IT-Systeme ist das ein Problem. Den Autoren sind Fälle bekannt, bei denen der Verantwortliche neue Paketfilterregeln auf eine Vielzahl von Rechnern verteilt hatte, die jeden Netzzugriff unmöglich machten. Dadurch war eine Rückkehr zur alten Konfiguration nur noch händisch an der Konsole möglich.

Die Einführung von Change-Management beinhaltet in der Regel die Delegation der Verantwortung für alle Änderungen an der IT-Infrastruktur durch die Unternehmensführung. Ab einem Zeitpunkt x dürfen alle zu betreuenden Systeme und Applikationen ausschließlich durch die Verantwortlichen und nur nach definierter Vorgehensweise geändert werden. Häufig nutzen Unternehmen das Change-Management gleichzeitig, um die Voraussetzungen für die Erfüllung heutiger gesetzlicher und branchenspezifischer Vorgaben (Compliance) zu schaffen.

Es empfiehlt sich, bei der Einführung einheitliche interne Begriffe festzulegen, da diese häufig sehr unterschiedlich benutzt werden. Definieren kann man etwa relevante Softwareänderungen wie Hotfixes, Sicherheits-Patches, integrierte Service-Packs et cetera. Bei der Modellierung des Prozesses selbst kann man sich an bestehenden Standards – unter anderem ITIL (IT Infrastructure Library [1]) – orientieren. Abbildung 1 zeigt den Ablauf des Prozesses.

Generell besteht der Change-Management-Prozess aus den drei Phasen Annahme, Planung und Steuerung. Zunächst erfassen die Verantwortlichen die Änderungsanforderung, filtern mehrfach eingereichte oder bereits früher abgelehnte Anforderungen heraus und akzeptieren die übrigen RfCs. Anschließend klassifizieren sie die gewünschte Änderung nach Priorität sowie Kategorie (Auswirkungen auf das Unternehmen und benötigte Ressourcen). Diese Klassifizierung ist die Grundlage für die Behandlung der Änderung – spätere Freigaben, besonders dringliche Behandlung et cetera.

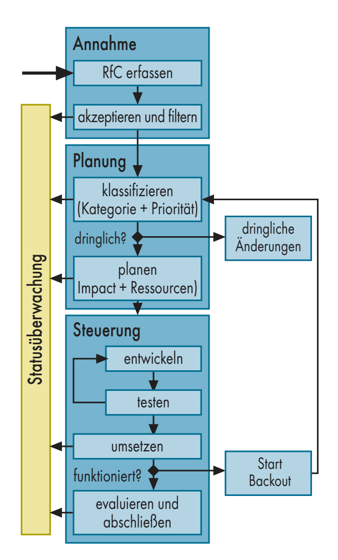
Durch die mit Change-Management verbundenen Arbeitsaufgaben entstehen neue Rollen und Gremien im Unternehmen, die personell zu besetzen sind. Zentrales Gremium ist dabei das Change Advisory Board (CAB). Es ist für die Akzeptanz des Change-Management-Prozesses unumgänglich, dass das CAB aus Vertretern aller von Änderungen betroffenen Organisationseinheiten besteht.

Beispielsweise kann das CAB aus Vertretern der Fachabteilung, Verantwortlichen der einzelnen Applikationen, der IT-Sicherheit, dem IT-Leiter, dem Verantwortlichen für Geschäftsfortführung (Business Continuity) und Notfallplanung sowie in jedem Fall dem Change Manager selbst bestehen. Seine Besetzung macht es unvermeidbar, dass die Beteiligten Kompromisse bezüglich der Interessen einzelner Mitglieder und den Geschäftszielen der Organisation als Gesamtheit schließen. Die häufigsten Konflikte entstehen bei der Wahl des geeigneten Zeitpunkts für das Umsetzen der Änderungen. Je nach Häufigkeit, Umfang und Komplexität der Änderungen kann das CAB anlassbezogen oder periodisch zusammenkommen. Regelmäßige Statusbesprechungen sind jedoch zu empfehlen, da durch das CAB eine Steuerung des Prozesses als Gesamtheit erfolgt.

Bei kleineren Unternehmen kann das CAB auch nur aus wenigen Personen bestehen, denn in solchen Organisationen besetzen einzelne Personen oft mehrere Rollen. Da die IT-Abteilung immer als Dienstleister im Change-Management-Prozess auftritt, ist es wichtig, dass mindestens ein Vertreter der von Änderungen oder Sicherheitserfordernissen betroffenen Fachabteilung(en) im CAB Mitglied ist. Das stellt sicher, dass Change-Management nicht zum Selbstzweck wird, sondern praxisnah auf die Geschäftsprozesse des Unternehmens ausgerichtet bleibt.

Entscheiden will gelernt sein

Eins der wichtigsten Elemente des Change-Management-Prozesses ist der erwähnte Request for Change. Er wird häufig als Formular in elektronischer oder Papierform erstellt und dient den Fach- und Stabsabteilungen wie der IT-Sicherheit zur Beantragung ihrer Ände-



Das Änderungsmanagement in einem Unternehmen sollte in genau festgelegten Schritten erfolgen, von der Annahme eines sogenannten „Request for Change" bis hin zur abschließenden Kontrolle – möglichst gesteuert durch eine eigene Organisationseinheit (Abb. 1).

iX-TRACT

- Da Änderungen an der IT nicht nur neue Soft- und Hardware, sondern verstärkt Updates und Sicherheits-Patches umfassen, steht und fällt die IT-Sicherheit eines Unternehmens mit der zeitnahen Durchführung der sogenannten Changes.
- Ohne festgelegte Change-Management-Prozesse unter der Kontrolle einer zuständigen Organisationseinheit geht es nicht – denn auch Software-Änderungen selbst sind eine Gefahr, wenn sie etwa unkontrolliert eingespielt werden und andere Anwendungen lahmlegen.
- Für Systeme, die regelmäßig zu aktualisieren sind, empfehlen sich fest installierte Testumgebungen mit standardisierten oder automatisierten Tests, deren zügige Durchführung eine Freigabe der Änderungen beschleunigt.

rungswünsche. Im weiteren Prozessverlauf findet eine Beurteilung durch den Change Manager statt, in komplexen oder umfangreichen Fällen müssen die CAB-Mitglieder ihre RfCs untereinander abstimmen. Viele Unternehmen etablieren gleich einen Abstimmungsprozess in Form eines zustimmenden Bewertungsworkflows für alle Betroffen und lassen den Change Manager am Ende der Kette auf der Basis der Anmerkungen eine Entscheidung treffen.

Der Workflow dient ebenfalls dazu, die Beteiligten über Art und Umfang der beantragten Änderung zu informieren oder sich darauf zu einigen – falls noch nicht erfolgt. Über diese Entscheidung werden dann alle Workflowteilnehmer und Betroffenen informiert. Kommt es zu keiner Einigung und kann der Change Manager auf der Grundlage der Anmerkungen keine Entscheidung treffen, so muss das CAB in seinem nächsten Treffen zu einer Einigung kommen oder sogar außerplanmäßig zusammentreten. Dies gilt auch, wenn die Verantwortlichen bei der Klassifizierung besonders umfangreiche Auswirkungen auf das Unternehmen feststellen oder solche, die große Ressourcen (Personal, Geld et cetera) erfordern.

Test für „Dauerbrenner“

Die beantragte Änderung wird anschließend in einen Umsetzungsplan integriert, geplant und durchgeführt. Dabei hängt der weitere Verlauf maßgeblich davon ab, ob lediglich ein vom Hersteller gelieferter Sicherheits-Patch zu installieren ist, eine Standardsoftware auf ihre Verteilung wartet oder gar ein eigenes Softwareentwicklungsprojekt durchgeführt werden muss.

Insbesondere in größeren Unternehmen hat sich in der Praxis die Verwendung sogenannter Standard-Changes bewährt. Das heißt, für Systeme, bei denen häufiger Änderungen zu erwarten sind – zum Beispiel Sicherheits-Patches für Windows-Arbeitsplatz-PCs – oder bei bis zu mehrmals täglichen Updates von Signaturen für einen Virenscanner sind permanente Testumgebungen zur Verfügung zu stellen. Für diese sind standardisierte beziehungsweise automatisierte Tests zu entwickeln, die bei positivem Ergebnis sofort eine Freigabe für die Änderungen an der IT-Infrastruktur nach sich ziehen. Dadurch lassen sich Abstimmungs- und Durchlaufzeiten für den Test der Changes deutlich verringern.

Heute gibt es bei den meisten Organisationen, die schon einen funktionierenden Change-Management-Prozess etabliert haben, noch erheblichen Optimierungsbedarf in der nachträglichen Qualitätssicherung der erfolgten Änderungen. Vernachlässigt wird in der Regel das unbedingt erforderliche Überprüfen der Änderungen nebst Dokumentation, ob die Änderung die vorher definierten Ziele erreicht hat. Ist das nicht der Fall, sollte man die Gründe dafür suchen und die Ergebnisse für die weitere Verbesserung des Prozesses verwenden.

Der Change-Management-Prozess kann durch Softwarewerkzeuge technisch unterstützt werden. Kauft man ein solches Werkzeug, lohnt sich eine sorgfältige Planung und Auswahl benötigter Funktionen. Die zentrale Bedeutung eines solchen Systems und seiner Teilsysteme erfordert außerdem die Entwicklung einer Sicherheitsrichtlinie für seinen Einsatz und seine sichere Konfiguration.

Die Notfallvorsorge beim Change-Management sollte ebenfalls durch einen geeigneten Mix aus technischen und organisatorischen Maßnahmen sichergestellt werden. Einerseits sind geeignete technische Redundanz- und Ersatzsysteme bereitzustellen, um einem nicht kompensierbaren Ausfall entgegenzuwirken. Andererseits sind Vertreterregelungen für die beteiligten Personen beziehungsweise ihre Rollen von Bedeutung, um den Entscheidungs- und Freigabeprozess aufrechtzuerhalten.

Kapazitäten gut planen

Beim Change-Management ist es auch unumgänglich, den Aspekt der Skalierbarkeit zu berücksichtigen. Die Hauptfaktoren, die die Skalierbarkeit beeinflussen, sind die geforderte Umsetzungsgeschwindigkeit für das Verteilen der Softwareänderungen auf die vorhandene IT-Infrastruktur und die Notwendigkeit, im Fehlerfall die IT-Systeme parallel wiederherzustellen. Bei der Auswahl eines technischen Systems sind diese als Voraussetzungen zu definieren und zu prüfen. Ebenso muss die vorhandene Netzwerkinfrastruktur bestimmte Anforderungen erfüllen, beispielsweise an die Bandbreite.

Möglicherweise sind zeitgleich mit der Softwareverteilung andere Anwendungen und Systeme (Netzwerk-Backup et cetera) mit ähnlichen Aufgaben und damit ähnlichem Verhalten im Netzwerk aktiv, was sich negativ auf die Dauer des Patch- und Änderungsprozesses auswirken kann. Die Umsetzungsgeschwindigkeit sollte der Verantwortliche daher sorgfältig bei den Tests vor Inbetriebnahme des Systems überprüfen. Auf eventuelle auftretende Engpässe in der IT-Infrastruktur muss er rasch durch Erweiterung oder Konfigurationsänderung reagieren.

In der Praxis hat es sich bewährt, die Skalierbarkeit entsprechend der physischen und geografischen IT-Struktur der Institution umzusetzen. Wenn es der Change-Management-Prozess des Unternehmens erlaubt, können beispielsweise in den verschiedenen Niederlassungen Verteilersysteme eingesetzt werden, die nur die Softwareänderungen für die IT-Systeme des jeweiligen Standortes erhalten und verarbeiten.

Anders als die Verfügbarkeit und Vertraulichkeit vernachlässigen Verantwortliche häufig die Sicherheitsziele Integrität und Authentizität bei Prozessen. Dabei sorgt eine erfolgreiche Integritätsprüfung dafür, dass die Dateien unverändert vorliegen, und eine positive Authentizitätsprüfung gewährleistet, dass eine Datei tatsächlich von derjenigen Quelle stammt, die sich als Absender ausgibt. Beide Aspekte sind sowohl für den Bezug der Softwareaktualisierungen von Herstellern als auch für den gesamten Patch- und Änderungsprozesses im Unternehmen wesentlich.

Nur geprüfte Pakete einspielen

Softwarehersteller verwenden häufig Prüfsummen oder Zertifikate, die die Integrität und Authentizität ihrer Softwarepakete sicherstellen sollen. Im Rahmen des Change-Management müssen die Verantwortlichen darauf achten, dass diese vor der Softwareaktualisierung stets überprüft werden. Bei negativem Ergebnis darf niemand die Softwareaktualisierungen installieren. Innerhalb des Change-Management ist festzulegen, mit welchen Werten die Prüfsummen zu vergleichen oder welche Zertifikate zu akzeptieren sind. So ergibt es beispielsweise wenig Sinn, kryptografische Prüfsummen vom selben Server herunterzuladen wie die Update-Pakete – was allerdings mehr die Regel ist als die Ausnahme [2]. Hat ein Angreifer den Server kompromittiert und Softwarepakete ausgetauscht, so kann er das ebenso leicht mit der zugehörigen Prüfsumme tun.

Ein weiterer Punkt, der zu regeln ist, sind Änderungen an mobilen Geräten wie Laptops, PDAs und Mobiltelefonen. Inzwischen existieren sogar Möglichkeiten, diese

Geräte über die Funkschnittstelle mit Updates zu versorgen – dabei ist allerdings die Instabilität der Verbindung und ihre geringe Bandbreite zu berücksichtigen. Dies gilt insbesondere dann, wenn der Benutzer vor einer Änderung noch die Daten auf dem Gerät sichern muss.

Der Change-Management-Prozess sollte ebenfalls Autoupdate-Mechanismen von Software berücksichtigen und vorgeben, wie mit ihnen zu verfahren ist. In der Regel enthalten heute alle Betriebssysteme und verfügbaren Standardsoftwarepakete solche Mechanismen. Ihre Aktivität, Konfigurierbarkeit, Administrations- und Benutzerunterstützung ist je nach Version, Installationsmodus und Hersteller unterschiedlich. Häufig fragen Hersteller außerdem unnötig viele Informationen vom verbundenen IT-System ab. Üblich ist die Abfrage von einem öffentlichen Updateserver nach neuen Versionen oder Softwarepaketen bei jedem Systemstart oder der Verbindung ins Internet.

Softwareprodukte bieten verschiedene Möglichkeiten, den Autoupdate-Mechanismus zu konfigurieren. Nicht jede Software erlaubt das vollständige Deaktivieren, oft bleibt nur die Wahl, mit eingesetzter Sicherheitssoftware die Abfrage zu unterbinden. Es gibt jedoch auch sinnvolle Anwendungsfälle – etwa die häufig anzutreffende Parallelkonfiguration bei mobilen Nutzern, die nicht immer innerhalb des Unternehmensnetzes arbeiten. Je nach Strategie des Unternehmens können die Verantwortlichen jedoch auch bestimmen, dass sämtliche Änderungen ausschließlich durch die interne Softwareverteilung erfolgen. Aus der Perspektive der Sicherheit ist abzuwägen, welches Vorgehen geringere Risiken mit sich bringt.

Fazit

Ein geregelter, gut durchdachter Change-Management-Prozess bringt neben großem Nutzen aus betrieblicher Sicht auch viele Vorteile in Sachen IT-Sicherheit. Insbesondere, wenn die Verantwortlichen die Zuständigen für IT-Sicherheit frühzeitig über anstehende Änderungen informieren und miteinbeziehen. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat daher beschlossen, neben der schon in den IT-Grundschutzkatalogen enthaltenen Maßnahme „Änderungsmanagement“ einen kompletten Baustein zum Thema „Patch- und Änderungsmanagement“ zu erstellen. Dieser Baustein wird unter anderem zahlreiche Hinweise und Informationen enthalten, wie man ein Change-Management sicher gestalten kann. (ur)

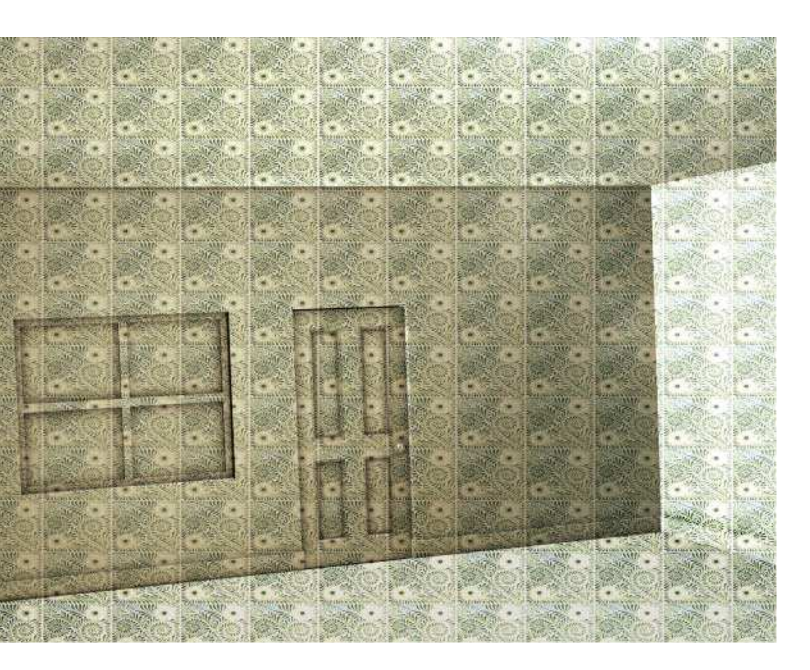
RONNY FRANKENSTEIN UND WILHELM DOLLE

arbeiten als Sicherheitsberater bei der HiSolutions AG in Berlin und erstellen zurzeit in Zusammenarbeit mit dem BSI den Baustein „Patch- und Änderungsmanagement“.

Literatur

[1] Michael Kuschke; IT-Services; Frisch auf den Tisch; Die dritte Version von ITIL; *iX* 9/2007, S. 139

[2] Michael Hamm; Kryptografie; Check oder Schreck; Hash-Funktionen unter der Lupe; *iX* 12/2007, S. 110



Daten in der Host Protected Area aufspüren

Gut versteckt

Christian Lange

Auf die im ATA-Standard für Konfigurationsdaten, Backup et cetera reservierte Host Protected Area soll der Benutzer nicht zugreifen können – doch Kriminelle scheren sich selten um Verbote oder Standards. Ermittler sollten daher wissen, wie sie die HPA nach Spuren oder versteckten Daten durchsuchen können.

Bei der Analyse von Computern oder Datenträgern, die im Zusammenhang mit Delikten stehen, müssen Ermittler diese möglichst vollständig auf Indizien und Spuren untersuchen – nicht immer ein einfaches Unterfangen, denn auf Rechnern gibt es Bereiche, in denen man Daten vor fremden Augen und Zugriffen verstecken kann. Ein solcher ist die Host Protected Area (HPA). Bei ihr handelt es sich um einen Bereich, der aus beliebig vielen Sektoren am Ende einer ATA/SATA-Festplatte bestehen kann. Charakteristisch an ihm ist, dass er dem Betriebssystem verborgen bleiben und so vor versehentlichem Formatieren, Löschen oder Partitionieren geschützt sein soll (siehe *iX*-Extra „Mobility“ in Ausgabe 6/2007) Dem ATA/ATAPI-4-Standard, der diese Funktion einführte, ist zu entnehmen, dass die HPA etwa zum Ablegen von Konfigurationseinstellungen gedacht war.

Verwendung findet die HPA beispielsweise heute bei einigen Notebooks als Rescue-Bereich, aus dem beim Booten nach Drücken einer speziellen Tastenkombination eine Anwendung startet, die ein Wiederherstellen beziehungsweise eine Neuinstallation des Betriebssystemes von dort aus ermöglicht. Des Weiteren gibt es Wiederherstellungsprogramme wie Phoenix FirstWare Recover Pro, die eine HPA einrichten und dort die Backups ablegen.

Damit Ermittler den Originaldatenträger bei der forensischen Untersuchung nicht verändern, führen sie diese grundsätzlich am bitweise kopierten Image der zu untersuchenden Festplatte durch. Die Erstellung dieser Imagedateien erfolgt in der Regel unter Verwendung eines Schreibschutzes entweder mit Varianten des Linuxbefehls *dd* (*dd_rescue*, *dcfldd*, *sdd*) oder mit gängigen forensischen Softwarewerkzeugen (AccessData FTK Imager, Guidance EnCase, Guidance LinEn, X-Ways Replica et cetera).

Befehle nicht weitergereicht

Nun sollte man annehmen können, dass diese Werkzeuge eine eventuell vorhandene HPA erkennen und bei der Sicherung einschließen. Aufgrund mehrerer Faktoren trifft das leider nicht automatisch zu. Schnittstelle (ATA/SATA) der Festplatte, Typ des Schreibschutzes beziehungsweise der Bridge (ATA auf USB, ATA auf SCSI oder ATA auf Firewire) spielen dabei die entscheidende Rolle.

„Normale“ Bridges wie die oben genannten reichen die für den Zugriff auf die HPA notwendigen ATA-Befehle im Allgemeinen nicht an die angeschlossene Festplatte weiter. Daher können Sicherheitswerkzeuge entgegen Herstellerangaben eine eingerichtete HPA nicht erkennen und deaktivieren. Sie beziehungsweise die in ihr gespeicherten Daten lassen sich nur dann mitsichern, wenn die Festplatte die relevanten ATA-Befehle auch erhält – das heißt im Umkehrschluss, dass die Festplatte entweder direkt an eine ATA-Schnittstelle oder über eine Bridge oder einen Schreibschutz, die über die Funktion des temporären Deaktivierens der HPA verfügen, angeschlossen sein muss.

Wie man eine HPA erkennt

Bevor man die Host Protected Area sichern kann, muss man erst einmal erkennen, dass sie vorhanden ist. Das kann durch einen Vergleich der auf der Festplatte genannten Sektorenanzahl mit derjenigen, die das forensische Werkzeug zur Sicherung anbietet, geschehen. Findet die Sicherung unter einem Linux-Betriebssystem statt, hilft bei ATA-Festplatten ein Blick in die Statusinformationen des Kernels mit dem Befehl *dmesg*:

```
hda: Host Protected Area detected.
     current capacity is 77091584 ↵
                    sectors (39470 MB)
     native  capacity is 78140160 ↵
                    sectors (40007 MB)
hda: Host Protected Area disabled.
```

Aktuelle Linux-Kernel deaktivieren eine eventuell eingerichtete HPA automatisch temporär, falls die Festplatte direkt an die ATA-Schnittstelle angeschlossen ist – wie es zum Beispiel beim Sichern mit der forensischen Boot-CD „Helix“ der Fall ist. Leider funktioniert das nicht bei SATA-Festplatten, da sie unter Linux als SCSI-Geräte angesprochen werden.

Benutzt der Ermittler bei der Sicherung einen Schreibschutz der Firma Tableau, hilft der „Tableau Disk Monitor“ beim Erkennen einer HPA (siehe Abbildungen 1 und 2). Alle Varianten (T5, T3u, T345 Ultrabay, T14 jeweils mit Firmware vom

09.07.2007) deaktivieren HPAs auf ATA- und SATA-Festplatten zuverlässig und zwar unabhängig vom zur Sicherung verwendeten Betriebssystem. Einen Hinweis auf eine vorhandene und temporär deaktivierte HPA erhält der Forensiker jedoch nicht automatisch – weder unter Linux noch mit der forensischen Software.

Verschlüsselung weckt Argwohn

Warum kompliziert, wenn es auch einfach geht. Zugegebenermaßen ist es leichter, Daten mithilfe von Verschlüsselungstechniken, etwa der Open-Source-Software Truecrypt zu verstecken. Der Einsatz von solcher Software ist jedoch auffällig und weckt das Misstrauen sowie den sportlichen Ehrgeiz des Forensikers. Bei der Verwendung einer HPA jedoch besteht die Möglichkeit, dass sie übersehen wird.

Der Umstand, dass Linux bei ATA-Festplatten die HPA nicht berücksichtigt, erleichtert deren Nutzung. Da jedoch ein Eintrag in der Partitionstabelle zu auffällig wäre, verzichtet darauf, wer kein Aufsehen erregen will, mit folgendem Trick:

```
losetup -o 39470899200 -s ⁊
        536832000 /dev/loop0 ⁊
                      /dev/hda
mkfs.ext3 /dev/loop0
mount /dev/loop0 /mnt/secret
```

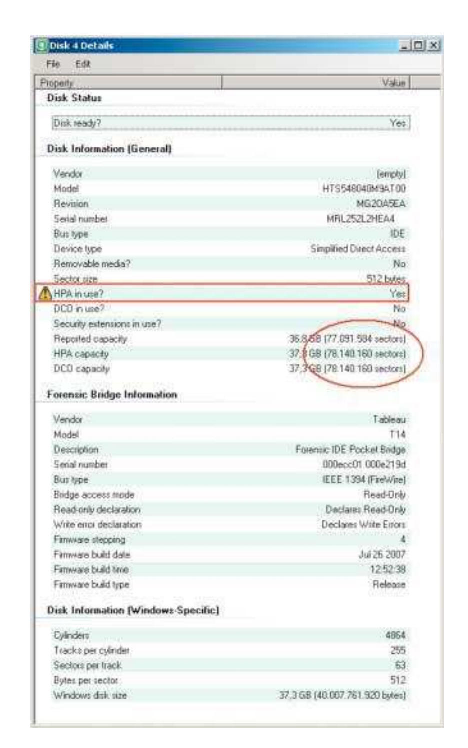
Diese drei Befehle reichen aus, um ab Byte-Offset 39470899200 einen zusammenhängenden Bereich von 536832000 Bytes an das Loopback-Device /dev/loop0 zu mounten, dann ein ext3-Filesystem darauf zu erzeugen, das auf den Mountpoint /mnt/secret gemountet wird. In diesem Beispiel kann man gut 500 MByte am Ende einer 40-GByte-Festplatte nutzen, nachdem dieser Bereich zuvor – mit *setmax.c* oder *HDAT2* – als HPA eingerichtet wurde [1, 2].

Zu empfehlen ist für den Ermittler in jedem Fall die Verwendung eines Schreibschutzes, der eine eventuell vorhandene HPA erkennen und temporär deaktivieren kann. Stehen diese nicht zur Verfügung, ist das Mitsichern einer HPA schwieriger. Es empfiehlt sich in diesen Fällen bei ATA-Festplatten, mit forensischen Linux-Boot-CDs wie Helix zu arbeiten.

Bei SATA-Festplatten sind DOS-basierte forensische Startdisketten/-CDs zu benutzen, die dann den Einsatz von beispielsweise X-Ways Replica erlauben. Es ist ebenfalls möglich, in diesen Fällen mit Werkzeugen wie HDAT2 zu arbeiten – jedoch sollte der ermittelnde Benutzer zunächst den Nachweis darüber führen, dass diese forensisch sauber arbeiten.



Der Schreibschutz von Tableau weist in seinem Disk Monitor auf das Vorhandensein einer Host Protected Area hin (rot eingerahmt) (Abb. 1).



Detailinformationen zur via Tableau angeschlossenen Festplatte: Auffällig ist hier die Differenz zwischen „Reported Capacity“ und „HPA Capacity“ – ein Indiz für die Nutzung der HPA (Abb. 2).

Fazit

Eine HPA kann, sofern ein Ermittler nicht explizit darauf achtet, leicht übersehen werden. Argumente wie „Wer kann die schon nutzen“ oder „Verschlüsselung ist einfacher“ dürfen nicht darüber hinwegtäuschen, dass das Einrichten und Nutzen einfach ist.

Nach Einschätzung des Autors verhält es sich mit der HPA wie bei einem sogenannten Kontrolldelikt – erst wenn man gezielt danach sucht, kann man sie auch finden. Daher sollte die Suche standardmäßig zur Ermittlung gehören. (ur)

CHRISTIAN LANGE

ist IT-Forensik-Spezialist in Niedersachsen.

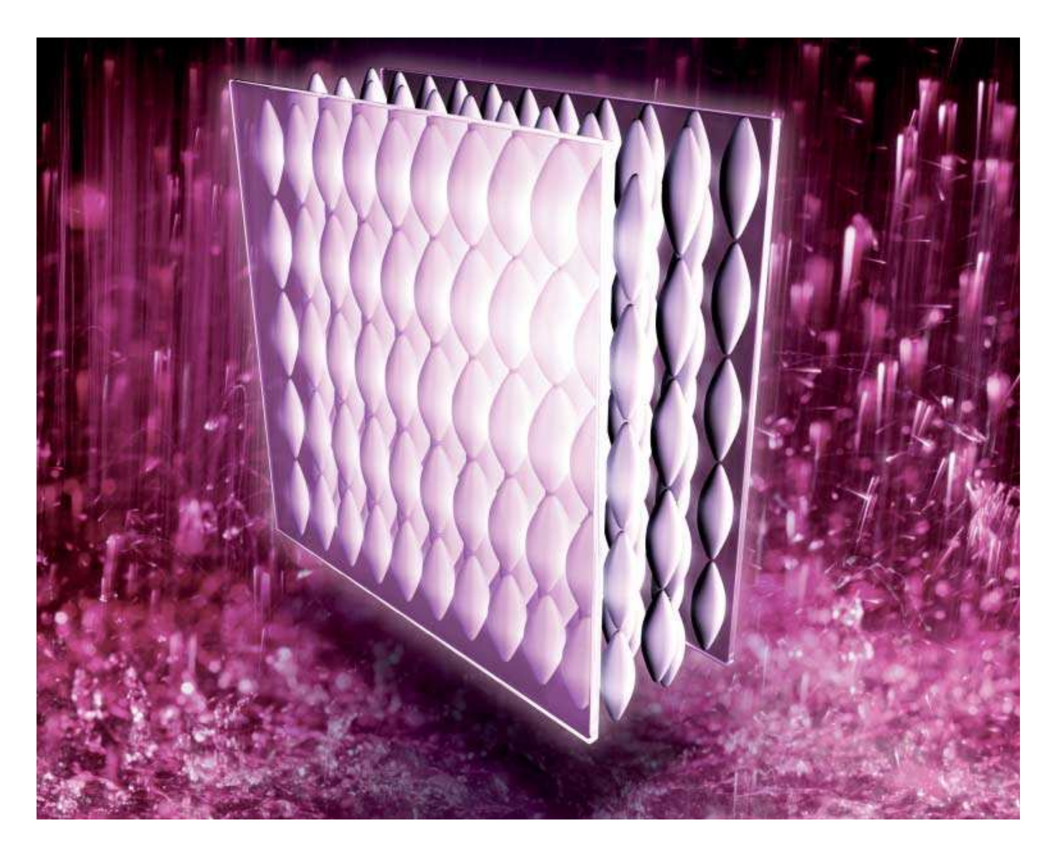
Literatur

[1] Oliver Tennert; Dateisystemforensik; In letzter Minute; Post-mortem-Analyse von Filesystemen unter Linux; *iX* 3/2006, S. 38

[2] Sebastian Krause; Computerkriminalität; Verdeckte Ermittlung; Shadow 2: Forensik-Hardware zur Systemanalyse; *iX* 10/2006, S. 72

Onlinequellen

AccessData Forensic Toolkit	www.accessdata.com
Guidance Encase Forensic Software	www.guidancesoftware.com
ATA-Tool HDAT2	www.hdat2.com
Helix Incident Response & Computer Forensics Live CD	www.e-fense.com/helix
Phoenix FirstWare Recover Pro	www.phoenix.com
Quellcode für HPA-verwandte ATA-Kommandos, *setmax.c*	www.win.tue.nl/~aeb/linux/setmax.c
Tableau, Schreibschutz	www.tableau.com
The Penguin Sleuthkit	www.sleuthkit.org/informer/sleuthkit-informer-20.txt
X-Ways Forensics, X-Ways Replica	www.x-ways.net



Die Technik hinter Projektoren und Groß-Displays

Kristall und Spiegel

Dieter Michel

Wer Inhalte per Projektor oder über ein großes Display vermitteln will, legt Wert darauf, dass die Wiedergabe der übermittelten Daten in guter Qualität erfolgt. Um eine hohe Auflösung, guten Kontrast und optimale Helligkeit zu gewährleisten, haben die Hersteller verschiedene Methoden entwickelt.

Für großflächige digitale Darstellungen stehen dem Anwender sowohl Projektoren als auch Displays mit einer Bilddiagonale von 40 Zoll und mehr zur Verfügung. In beiden Marktsegmenten haben die Hersteller unterschiedliche Verfahren für die Bildwiedergabe entwickelt.

Bei Projektoren unterscheidet man zwischen LCD, LCoS und DLP. Die Bild-Erzeugung bei LCD-Geräten (Liquid Crystal Display) funktioniert wie beim Computermonitor: Im LCD-Panel befindet sich zwischen zwei Glasplatten mit aufgedampften Elektroden eine dünne Flüssigkristallschicht. Deren Moleküle sind anisotrop, haben also eine ausgezeichnete Richtung und wirken deshalb doppelbrechend. Beleuchtet man die Flüssigkristallschicht mit polarisiertem Licht, wird die Polarisationsebene beim Durchgang durch das LC-Medium gedreht.

Um diesen Effekt für Display-Zwecke nutzbar zu machen, hat man ein Verfahren entwickelt, das die Flüssigkristallmoleküle mit einer sogenannten Alignment-Schicht auf den inneren Glasoberflächen ausrichtet. Da die Moleküle elektrisch polar sind, orientieren sie sich entsprechend ihren Nachbarn. Sind die Vorzugsrichtungen der Alignment-Schichten parallel beziehungsweise gekreuzt orientiert, richten sich die LC-Moleküle parallel respektive schraubenförmig aus und drehen die Polarisationsebene des einfallenden Lichts dementsprechend.

Durch einen zweiten Filter hinter dem Panel kann man nun diese Verdrehung der Polarisationsebene in Helligkeitsunterschiede umsetzen. Je nach Orientierung dieser Ebene zur Vorzugsrichtung des Polfilters wird Licht durchgelassen (0°, parallel), gesperrt (90°, gekreuzt) oder mehr oder weniger stark abgeschwächt (Zwischenwerte). Abhängig von der Ausrichtung der Vorzugsrichtungen der beiden Alignment-Schichten und der Polfilter kann man Displays bauen, die im Ruhezustand Licht durchlassen oder sperren.

Als Display nutzbar ist das Ganze erst, wenn man das Durchlassverhalten von außen steuern kann. Das geschieht über die erwähnten, fast völlig transparenten Elektroden auf den Glasflächen. Eine zwischen ihnen angelegte Spannung erzeugt ein elektrisches Feld, das auf die Orientierung der Flüssigkristallmoleküle wirkt. Je nach Spannung kann das LCD-Panel Licht mehr oder weniger stark durchlassen. Die Steuerkennlinie ist nichtlinear, was die Ansteuerelektronik intern kompensiert.

Subpixel einzeln ansteuern

Bildgebend wird die LCD-Technik durch die Aufteilung des Panels in einzelne Pixel beziehungsweise Subpixel, deren Ansteuerung individuell erfolgt. Bei praktisch allen heutzutage verkauften Projektoren geschieht das mit der TFT-Technik. TFT steht kurz für Thin Film Transistor und besagt, dass jedes Subpixel, also jede einzelne Zelle des LCD-Panels, eine eigene kleine Transistorschaltung hat, die individuell adressierbar ist und bis zum nächsten Update die programmierte Ansteuerspannung hält. Das funktioniert, weil nur ein elektrisches Feld erzeugt wird und

kein Strom fließen muss. Dank moderner Dünnfilmtechnik (Thin Film Technology) kann der pro Zelle erforderliche Transistor sehr klein sein, aber er muss sich in unmittelbarer Nähe der Zelle befinden und ist demzufolge zwangsläufig mit im Bild.

Kristalle modellieren das Licht

LCoS steht kurz für Liquid Crystal on Silicon und ist eine Variante der LCD-Technik. Die Lichtventilfunktion arbeitet hier ähnlich wie bei LCD, jedoch wird das Panel nicht durchstrahlt, sondern arbeitet reflexiv. Der Schichtaufbau des Panels besteht – von der Panelvorderseite aus gesehen – aus Polarisationsfilter, Glasplatte, Flüssigkristallschicht und der Rückseite. Diese enthält die Ansteuerschaltungen, die im Prinzip wie bei einem LCD-Panel funktionieren, sich aber hinter der reflektierenden Oberfläche befinden. Der Transistor liegt daher nicht mehr im Lichtweg, sodass der Füllfaktor der Pixelfläche hoch ist – meist über 90 Prozent – und die Lücken zwischen den Pixeln sehr schmal sind. Den Fliegengittereffekt gibt es bei LCoS daher praktisch nicht. Durch eine Metallisierung der Rückelektrodenoberfläche – meist Aluminium – kann diese gut reflektieren. Die eigentlichen Elektroden bestehen aus Silizium, daher die Bezeichnung Liquid Crystal on Silicon.

Da mit zunehmender Panel-Auflösung und mithin kleineren Pixeln die Ansteuertransistoren nicht extrem klein werden müssen, weil sie nicht im Lichtweg liegen, kann man mit der LCoS-Technik gut hochauflösende Displays bauen. LCoS arbeitet mit einer Flüssigkristallschicht als Lichtmodulator, sodass bezüglich der Langzeitstabilität sinngemäß dasselbe gilt wie bei LCD-Panels.

DLP, das Digital Light Processing, hingegen funktioniert durch das Verkippen einer großen Menge extrem kleiner Spiegel. Bei einem 50 Zoll großen Digital Mirror Device (DMD) in XGA-Auflösung zum Beispiel steht für ein Pixel eine quadratische Fläche von lediglich 10,9 μm Kantenlänge zu Verfügung. Und darauf gilt es, nicht nur den Spiegel selbst, sondern zudem eine mechanische Lagerung sowie eine Art Antrieb für das Kippen der Spiegel unterzubringen.

Spieglein, Spieglein auf dem Chip

Man kann die Realisierung dieser Anforderungen als ein Musterbeispiel für mikromechanische Konstruktionen auf der Basis moderner Chipfertigung begreifen. Als Grundbaustein des DMD dient eine mikromechanische Struktur, die aus einem Spiegel besteht, der starr mit einem darunterliegenden Träger verbunden ist. Dieser Träger ist wiederum mit zwei dünnen Torsionsbändern auf Pfosten befestigt, die sich auf der Substratbasis befinden. Träger dieser Struktur ist ein normaler CMOS-Baustein, dessen Speicherzellen mit passendem mechanischen Rastermaß direkt unter den Spiegeln liegen. Je nach Inhalt der Speicherzellen entstehen elektrostatische Felder zwischen dem Spiegel beziehungsweise Spiegelträger und der darunterliegenden Speicherzelle, die eine Drehung des Spiegels in positiver oder negativer Richtung bewirken. Die Drehbewegung wird durch mechanische Anschläge (landing pads) je nach DMD-Chip auf +/- 10° beziehungsweise +/- 12° begrenzt .

Die Herstellung der DMD-Struktur beginnt mit der mehr oder weniger normalen Fertigung eines CMOS-Speicherbausteins. Nicht weniger als sechs Fotomasken bilden dann die Spiegelstruktur mit Aluminiumschichten für die Adresselektrode, die Torsionsbänder, das Scharnier, den Spiegelträger und die Spiegelschichten. Durch eine Kathodenzerstäubung (Sputtern) werden die Aluminiumschichten aufgebracht und im Plasmaätzverfahren strukturiert. Sogenannte „Opferschichten“ halten die Luftspalte, die später den Bewegungsspielraum der Spiegel ermöglichen, bei der Herstellung frei. Ein weiterer Schritt ätzt diese Schichten weg und gibt so die Spiegelchen frei. Eine einzelne Zelle dieser Struktur ist nicht größer als circa 10 × 10 μm und beträgt somit nur knapp ein Fünftel der durchschnittlichen Dicke eines menschlichen Haars.

Wie Farbe ins Spiel kommt

Am Ende des Prozesses entstehen so mechanisch bewegliche Spiegelflächen aus Aluminium, die über dünne Torsionsbänder mit dem Substrat verbunden sind. Diese Bänder sind so fein und die Auslenkwinkel klein genug, dass die Bewegung der Torsionsbänder rein elastisch bleibt und nicht in den Bereich plastischer Verformung gerät. Daher tritt innerhalb der Lebensdauer des DMD-Chips interessanterweise keine nennenswerte Materialermüdung auf, die etwa zum Ausfall einzelner Pixel führen könnte.

Der Lichtablenkmechanismus allein kann nur weiße und schwarze Pixel erzeugen. Die Erzeugung eines farbigen Bildes mit Helligkeitsabstufungen erfordert zwei zusätzliche Komponenten.

Für die Helligkeitsabstufungen ist die Ansteuerung der Spiegelchen zuständig.

Das reine Kippen der Spiegel erfolgt über das Schreiben entsprechender Bitmuster in den CMOS-Speicher. Dieser Vorgang legt ein elektrisches Feld zwischen dem Spiegel und den unter zwei gegenüberliegenden Ecken des Spiegels befindlichen Speicherzellen an. An den anderen beiden Ecken elastisch gelagert, kippt der Spiegel durch die Anziehungskraft des elektrischen Feldes in die gewünschte Richtung.

Eine Pulsbreiten-Ansteuerung erzeugt Helligkeitsabstufungen. Je länger der Spiegel innerhalb einer Bildperiode Licht in Richtung Objektiv lenkt, desto heller erscheint der betreffende Bildpunkt. Für 256 Helligkeitsstufen (8 Bit) und eine interne Bildfrequenz von 60 Hz benötigt man also eine Zeitauflösung von circa 65 µs (entsprechend 15,36 kHz).

Auf diese Weise entsteht zunächst nur ein Graustufenbild. Für die Erzeugung von Farbbildern kennt die DLP-Technik zwei Verfahren: Man kann das weiße Lampenlicht mit dichroitischen Filtern (Dichroismus = Zweifarbigkeit von Kristallen beim Lichtdurchgang, hier: Farbtrennung von reflektiertem und durchgelassenem Licht an Interferenzfiltern) in drei Grundfarben beziehungsweise Lichtwege aufteilen und dann drei DLP-Chips benutzen, um diese Farben parallel zu verarbeiten und anschließend wieder zusammenzuführen. Wegen der vorgegebenen Ablenkwinkel ist der Lichtweg allerdings kompliziert, und da zudem der Bedarf an drei DLP-Chips eine solche Konstruktion teuer macht, kommt sie nur in High-End-Projektoren und solchen mit hoher Lichtleistung zum Einsatz.

Bei Weitem üblicher ist der Betrieb im Zeitmultiplex. Das geht bei DLP, weil die Schaltzeiten der Spiegel sehr niedrig sind. Dadurch lassen sich innerhalb einer Bildwechselperiode (1/60 s) die drei Grundfarben Rot, Grün und Blau nacheinander erzeugen. Das menschliche Auge integriert normalerweise die drei Teilbilder und nimmt nur ein einziges, farbiges Bild wahr.

Um den Spiegelchip nacheinander mit den Grundfarben Rot, Grün und Blau zu beleuchten, verwenden Hersteller normalerweise ein Farbfilterrad, das aus Filtersegmenten in den drei Grundfarben und gegebenenfalls zusätzlich Weiß zusammengesetzt ist. Es befindet sich im Strahlengang zwischen Lampe und DMD-Chip und filtert jeweils die gewünschte Farbe aus dem weißen Lampenlicht heraus.

Nach und nach die Grundfarben

Das Filterrad dreht sich mit einer Umdrehung pro Bildwechselperiode, es fällt also nacheinander Licht in den drei Grundfarben auf den Spiegelchip. Steuert man die Spiegelchen synchron nun mit der Filterraddrehung entsprechend der Helligkeitsverteilung des Bildes für die jeweilige Grundfarbe an, werden nacheinander die drei RGB-Farbauszüge des farbigen Bildes auf die Leinwand projiziert.

LC-Displays funktionieren im Prinzip wie die LCD-Panels in Projektoren und Computerbildschirmen. Zwischen zwei Glasplatten mit aufgedampften Elektroden befindet sich eine Flüssigkristallschicht, die doppelbrechend und daher in der Lage ist, die Ebene von polarisiertem Licht zu drehen.

Filter sorgen für ein gerastertes Bild

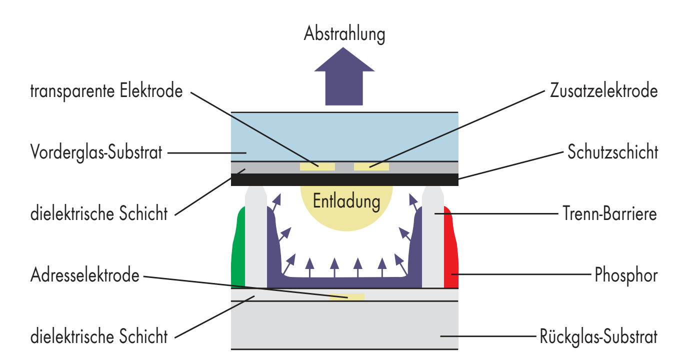
In Displays kommt das Licht meist von einer Backlight-Unit, die mit Kaltkathoden-Leuchtstoffröhren arbeitet und eine flächige Hintergrundbeleuchtung bereitstellt. Polarisationsfilterfolien im Strahlengang vor und hinter der Flüssigkristallschicht sorgen für die lineare Polarisation des Lichts und die Umsetzung des Drehwinkels in einen Helligkeitsunterschied. Eine Aufteilung in farbige Subpixel sorgt über Filter in den Grundfarben letztendlich für ein gerastertes, farbiges Bild. Auch hier gibt es pro Subpixel einen Transistor zur Ansteuerung der Zelle. Schwierig ist das bei einem Groß-Display aber nicht, weil der Transistor ja nicht durch eine Projektion vergrößert dargestellt wird.

Die Funktionsweise eines Plasma-Displays ist grundlegend anders als die eines LC-Geräts, deshalb sind die Vor- und Nachteile ebenfalls anders gelagert. Ein Plasma-Display besteht aus einzelnen Zellen – für jedes farbige Subpixel eine –, die in Zeilen und Spalten entsprechend der nativen Auflösung des Displays angeordnet sind. Den Aufbau einer einzelnen Zelle zeigt Abbildung 1.

Die Zelle ist hinten sowie an den Seiten durch feste Wände begrenzt und nach vorn durch eine Glasscheibe abgeschlossen. Auf dieser Glasscheibe sind Elektroden aufgedampft, der Innenraum der Zelle ist mit einem speziellen Gasgemisch unter niedrigem Druck gefüllt. Wird zwischen den Elektroden eine genügend hohe Spannung angelegt, löst dies eine energiereiche Gasentladung (Plasma) aus. Diese Entladung strahlt auch Licht ab, allerdings vorwiegend im Bereich kurzer Wellenlängen (UV), was bewirkt, dass sie selbst fast unsichtbar ist. Ähnlich wie bei einer Leuchtstoffröhre setzt man deshalb mithilfe eines Leuchtstoffs das fast unsichtbare UV-Licht der Plasmaentladung in längerwelliges, also sichtbares Licht um (Fluoreszenz).

Quantenausbeute spielt eine Rolle

Welche Farbe das vom Leuchtstoff ausgestrahlte Licht hat, hängt von der chemischen Zusammensetzung des Leuchtstoffs ab. Hier hat man als Entwickler nicht ganz die freie Wahl, weil auch Aspekte wie die Quantenausbeute eine Rolle spielen (Bei wie viel Prozent der absorbierten Photonen wird wieder ein Photon ausgestrahlt?). Schließlich möchte ja jeder Hersteller einen möglichst hellen, energieeffizienten Monitor bauen. Die Leuchtstoffe sind beim Plasma-Display auf der Rückwand und auf den Seitenwänden der Zelle aufgebracht, sodass das erzeugte Licht ungehindert nach vorn durch die Abdeckscheibe austreten kann. Da der Leuchtstoff annähernd ein diffuser Strahler ist, gibt es bei diesen Geräten nahezu keine nennenswerte Abhängigkeit des Bildkontrasts und der Farbwiedergabe vom Blickwinkel. (ka)



Für jedes farbige Subpixel verfügt ein Plasma-Display über einzelne Zellen (Abb. 1).

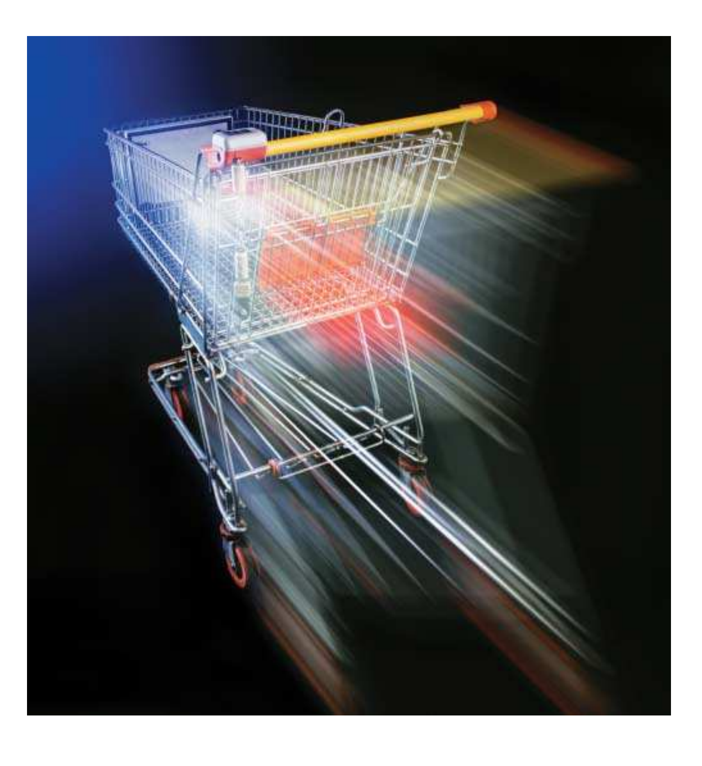
DIETER MICHEL

arbeitet als freier DV-Journalist und ist Chefredakteur der Fachzeitschrift Prosound.

SPECjms2007 misst Message Oriented Middleware

Kaffeekunde

Samuel Kounev, Kai Sachs



Offensichtlich wächst der Bedarf an Messwerkzeugen für die Leistungsfähigkeit von Java-Applikationen in der Wirtschaft, denn die SPEC, eine internationale Herstellervereinigung, hat eine dritte Klasse von Benchmarks für solche Umgebungen herausgebracht.



Da Java vor allem im geschäftlichen Bereich an Bedeutung gewonnen hat, sind für solche Umgebungen Werkzeuge gefragt, mit denen sich die Performance bestimmen lässt. Unter Federführung der Standard Performance Evaluation Corporation (SPEC – siehe Onlinequellen [a]), die aus über 80 Mitgliedern besteht – darunter alle namhaften Software- und Hardwarehersteller – entstand ein neuer Benchmark, der die Leistungsfähigkeit der Message Oriented Middleware (MOM) misst. Aufsetzend auf den Java Message Services (JMS) [b], nutzt der SPECjms2007 [c] das Modell der Lieferkette eines Supermarktes. Es ist der erste Benchmark für MOM.

Benchmark mit Analyseoption

SPECjms2007 baut ein Testszenario auf, das die Leistungsfähigkeit aller eingesetzten Komponenten der MOM, inklusive der Hardware, ermittelt. Als Ergebnis erhält der Anwender umfangreiche Berichte über das Verhalten des getesteten Systems sowie eine zusammenfassende Metrik. Die Berichte können als Grundlage für eine Investitionsentscheidung oder zur Analyse und Optimierung bestehender Infrastrukturen dienen. Um Last auf der MOM zu erzeugen, nutzt SPECjms2007 die standardisierte JMS-Schnittstelle, wie sie die MOM-Produkte namhafter Softwarehersteller unterstützen. Dazu zählen etwa die Java Enterprise Edition (JEE) sowie die Klassiker IBMs Websphere MQ und Tibco Enterprise Message Service. JMS hat sich damit als Quasi-Standard im Bereich MOM etabliert.

Durchführung und Ergebnisse der SPEC-Benchmarks unterliegen einer strengen Qualitätskontrolle. Bei der Entwicklung achtete das Gremium darauf, dass die Leistungsmessung eines Systems unter einer realitätsnahen Arbeitslast stattfindet. Nur so erhält das Ergebnis eine Aussagekraft über das reine Messen der Funktionen hinaus. Resultate von SPEC-Benchmarks dürfen die Tester erst veröffentlichen, nachdem das Protokoll einen Review-Prozess durchlaufen hat, bei dem es andere Hersteller und Konkurrenten penibel auf mögliche Ungereimtheiten und Regelverletzungen durchleuchten. Erst nach der Freigabe und der Veröffentlichung darf das betroffene Unternehmen die Resultate etwa für Marketing-Zwecke einsetzen. Unter anderem durch diese Form der Qualitätskontrolle haben SPEC-Benchmarks eine weltweite Akzeptanz erreicht. Sie bilden teilweise die Grundlage für Ausschreibungen.

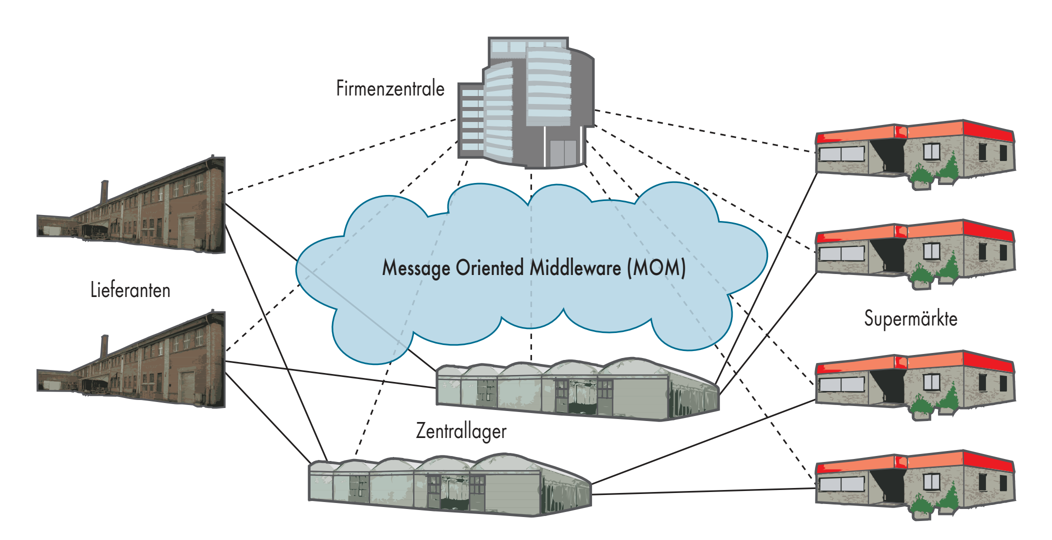
SPECs Klassen der Java-Benchmarks

Im Bereich Java hat SPEC bisher eine Reihe von Benchmarks veröffentlicht: für die „Java Virtual Machine“ den SPECjvm98 und den für nächstes Jahr angekündigten SPECjvm2008 [d], für serverseitige Java-Anwendungen den „Java Business Benchmark“ SPECjbb2005 [1, e] und für „Java Enterprise Edition Application Server“ den SPECjAppServer2004 [f]. Obwohl JMS ein Teil der JEE ist, versteht sich der SPECjms-2007 nicht als ein zweiter Benchmark für JEE-Produkte. Er soll der Tatsache Rechnung tragen, dass sich JMS als Schnittstelle für Enterprise MOM etabliert hat, was insbesondere Produkte jenseits der JEE einschließt. JMS hat als Basistechnik für serviceorientierte Architekturen (SOA) und Electronic Design Automation (EDA) eine große Bedeutung erlangt. Solche Architekturen verknüpfen die unterschiedlichen Anwendungen und Dienste innerhalb einer IT-Infrastruktur miteinander.

Deshalb ist ihre Performance und Skalierbarkeit von immenser Bedeutung für einen reibungslosen Ablauf.

iX-TRACT

- Mit SPECjms2007 steht erstmals ein Benchmark für Message Oriented Middleware zur Verfügung.
- Grundmodell ist der Informations- und Warenfluss in einer Supermarktkette.
- SPECjms2007 erlaubt den Vergleich sowohl von JEE-Produkten als auch von MOM-Umgebungen.



In Szene gesetzt: Der Nachrichtenfluss in der Supply-Chain einer Supermarkt-Kette liefert das Modell für den SPECjms2007. Durchgezogene Linien stehen für den Waren-, gestrichelte für den Informationsfluss (Abb. 1).

Es gibt seit Längerem einige Hilfsmittel zur Leistungsbestimmung für den Bereich. Meist handelte es sich um hintereinandergeschaltete Tests einzelner Funktionen der MOM, beispielsweise um Messungen mit einer bestimmten Nachrichtengröße ohne standardisierte Lastszenarien. Veröffentlichungen kamen hin und wieder zu teilweise widersprüchlichen Ergebnissen. Gründe hierfür sind häufig unterschiedliche Gewichtungen, variierende Rahmenbedingungen und mangelnde unabhängige Kontrollen. Um dem zu begegnen, entstand unter der Leitung der TU Darmstadt und der Mitwirkung von Firmen wie IBM, Sun, Bea, Oracle, Sybase, JBoss und ActiveMQ das SPECjms2007-Projekt.

Aktionen in der Handelskette

Im zugrunde liegenden Modell stellen die Supermärkte, Zentrallager (Distribution Center), Lieferanten (Supplier) und die Firmenzentrale (Headquarter) (Client-) Anwendungen dar, die über eine MOM Nachrichten untereinander austauschen. In einer solchen Umgebung spielen sich in der realen Welt eine Vielzahl von Interaktionen ab, angefangen bei Lagerbewegungen bis hin zu Wiederbeschaffungsmaßnahmen und dem Sammeln von Verkaufsstatistiken.

Der SPECjms2007 simuliert die Client-Anwendungen, zwischen denen sieben exemplarische Interaktionen ablaufen (siehe Tabelle „Sieben Aktionen im SPECjms 2007“), die jeweils andere MOM-Funktionen testen. Angefangen bei verschiedenen Nachrichtentypen und -größen über den Einsatz von Transaktionen deckt der Test einen Querschnitt der von JMS zur Verfügung gestellten Funktionen ab.

Über die Variation der Anteile der Interaktionen an der Gesamtlast lassen sich Lastszenarien modellieren, ein wesentlicher Unterschied des SPECjms2007 gegenüber bisherigen Benchmarks: Der Benutzer hat die Freiheit, sich seinen Ansprüchen entsprechende Lastszenarien zusammenzustellen, beispielsweise kann er die Anzahl von Artikeln pro Einkauf festlegen. Die Voraussetzung bietet ein komplexes Framework, das über 150 Konfigurationparameter hat. Solche frei definierten Szenarien sind für eigene Analysen und interne Tests gedacht. Messergebnisse, die darauf beruhen, sind nicht zur Veröffentlichung bei der SPEC geeignet.

Horizontal und vertikal gemessen

Neben diesem Freeform-Modus bietet der SPECjms2007 zwei weitere (horizontal und vertikal) mit eigenen Lastszenarien an, deren Ergebnisse der Tester einreichen kann. In beiden Fällen erhält man als Ergebnis eines Testlaufs eine BASE-Metrik. Sie kontrolliert die Gesamtlast auf dem System und somit die Anzahl der erzeugten Nachrichten. Eine höhere BASE entspricht einer höheren Last. Der Unterschied der beiden Modi besteht darin, wie es zur Erhöhung der Last kommt:

Im vertikalen Modus bleibt die Anzahl der Clients konstant, etwa die der Supermärkte. Eine höhere BASE erzeugt

Sieben Aktionen im SPECjms2007

Aktion	Beschreibung
1.	Bestellung eines Supermarkts bei einem Zentrallager und anschließende Lieferung der Ware
2.	Preisanfrage eines Zentrallagers bei verschiedenen Lieferanten mit anschließender Bestellung und Lieferung der Ware
3.	Übermittlung neuer Produktpreise durch die Firmenzentrale
4.	Erfassung von Lagerbewegung (durch RFID-Reader) und Aktualisierung des Lagerbestandes eines Supermarkts
5.	Übermittlung von Verkaufsstatistiken eines Supermarkts an die Firmenzentrale
6.	Ankündigung neuer Produkte durch die Firmenzentrale
7.	Übermittlung von Listen gesperrter/geklauter Kreditkarten durch die Firmenzentrale (sogenannte Hotlists)

Message Oriented Middleware

Die Kommunikation von Anwendungen untereinander koordiniert eine Message Oriented Middleware. Sie bildet unter anderem die Basis für eine Service Oriented Architecture (SOA) oder eine Event Driven Architecture (EDA) [2].

MOM stellt die Nachrichten asynchron zu und unterstützt zwei Formen der Kommunikation: Das Message-Queueing, bei dem die Kommunikation zwischen zwei Anwendungen über eine Warteschlange stattfindet, oder das Publish/Subscribe-Verfahren, bei dem Interessenten Nachrichten mit bestimmten Eigenschaften bei einer MOM abonnieren können [3].

Ein klassisches Beispiel für ein solches Abonnement sind die Börsenkurse eines bestimmen Unternehmens. Die Vorteile einer MOM liegen vor allem in der Skalierbarkeit und der Entkopplung von Nachrichtenproduzenten und -konsumenten.

höhere Last pro Client, beispielsweise durch mehr Verkäufe pro Supermarkt. Im Gegensatz dazu steuert die BASE im horizontalen Modus die Anzahl der Anwendungen, während die Nachrichtenlast pro Anwendung unverändert bleibt. Beispielsweise variiert die Zahl der Supermarkt-Filialen mit BASE, die Verkäufe pro Supermarkt bleiben hingegen gleich. Zusammengefasst kann man sagen, dass der vertikale Modus eine Umgebung mit wenigen Clients, aber einer hohen Last simuliert, während der horizontale Modus eine verteilte Umgebung mit vielen Clients abdeckt.

Fazit

Der Benchmark erlaubt nicht nur einen Vergleich verschiedener JEE-Produkte, sondern stellt solche Lösungen zum ersten Mal in direkte Konkurrenz zu klassischen MOM-Umgebungen. Damit stehen für den Bereich der Java-Applikationen im geschäftlichen Umfeld drei Benchmarks allein bei der SPEC zur Verfügung.

SPECjms2007 dürfte wie alle bisherigen Benchmarks der SPEC einen starken Einfluss auf die Optimierung und -weiterentwicklung von Produkten haben.

Wer den SPECjms2007 einsetzen möchte, sei es zur Analyse eigener Umgebungen oder um für das eigene Produkt Ergebnisse zu gewinnen und diese zu publizieren, muss 1800 US-$ bei der SPEC entrichten. Gemeinnützige und Bildungseinrichtungen zahlen nur 450 US-$. (rh)

Onlinequellen

[a]	SPEC-Site	www.spec.org
[b]	Java Message Service (JMS)	java.sun.com/products/jms/Standard
[c]	SPECjms2007	www.spec.org/jms2007/
[d]	SPECjvm98	www.spec.org/osg/jvm98/
[e]	SPECjbb2005	www.spec.org/jbb2005
[f]	SPECjAppServer	www.spec.org/jAppServer/

DR. SAMUEL KOUNEV

ist momentan Gastwissenschaftler an der Universität Cambridge und war als Projektmanager an SPECjms2007 beteiligt.

KAI SACHS

ist diplomierter Wirtschafts-Informatiker und als wissenschaftlicher Mitarbeiter an der TU Darmstadt tätig. Er war aktiv an der Entwicklung des SPECjms2007 beteiligt.

Literatur

[1] Ralph Hülsenbusch; Benchmarks; Kaufhauskette; Java Business Benchmark 2005: elektronische Warenhäuser als Test; *iX* 6/06, S. 112

[2] Alexander Schatten, Josef Schiefer; IT-Architekturen; Ungeplante Wege; Ereignisbasierte Systeme verbessern SOA; *iX* 7/07, S. 122

[3] Ian Gorton; Essential Software Architecture; Springer-Verlag, Berlin, Heidelberg; 2006



Datenvisualisierung mit Self-Organizing Maps

Kleine Inselmusik

Cai Ziegler

Mit Self-Organizing Maps lassen sich mehrdimensionale Daten gruppieren und grafisch reizvoll in Form von Hügeln, Tälern und Gewässern darstellen. Dieses medienwirksame Instrument, das gerade wieder in Mode kommt, macht selbst vor Mozarts Musik und Konterfei nicht Halt.

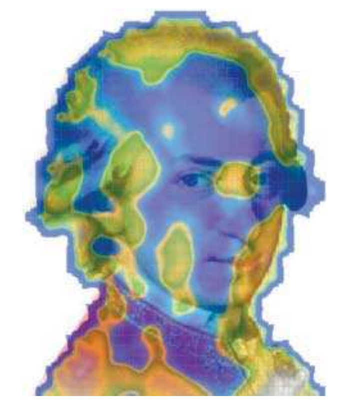
Als Teuvo Kohonen zu Beginn der Achtziger mit den Self-Organizing Maps, oft als Hommage an seine Leistung als Kohonen Maps bezeichnet, den großen Wurf seines Lebens tätigte, hätte er wohl nicht zu träumen gewagt, welch hohe Wogen seine bunten Kärtchen schlagen würden. So hohe, dass diese sozusagen buchstäblich über das erhabene Gesicht des ehrwürdigen Mozart schwappten (siehe Abbildung 1).

Zu dieser kuriosen Anwendung ließen sich im März letzten Jahres, pünktlich zum 250. Geburtstag des Virtuosen, einige Wissenschaftler der Technischen Universität Wien hinreißen. Die „Map of Mozart“ fand in zahlreichen Medien ihren Niederschlag, unter anderem in Geo [1] und bei Spiegel Online. Zunächst ist die Mozart-Karte nur eine über sein Antlitz geblendete Insellandschaft. Das Besondere dabei ist die Bedeutung der Inseln, denn jeder Archipel repräsentiert einen Satz von Mozarts Werken mit großer klanglicher Ähnlichkeit. Ergo handelt es sich um eine musikalische Landkarte, die der Musikbegeisterte erforschen kann, als wäre es die Welt und er ein darin Reisender. Gewässer trennen derartige Cluster ähnlicher Schaffenswerke voneinander und so finden sich beispielsweise Serenaden und Violinkonzerte auf eigenen Inseln. Das im Web befindliche interaktive Gesicht (siehe [a] in den „Onlinequellen“) erlaubt munteres Klicken auf der Karte und spuckt dabei Infos zu den Werken, die auf der selektierten Insel existieren, aus.

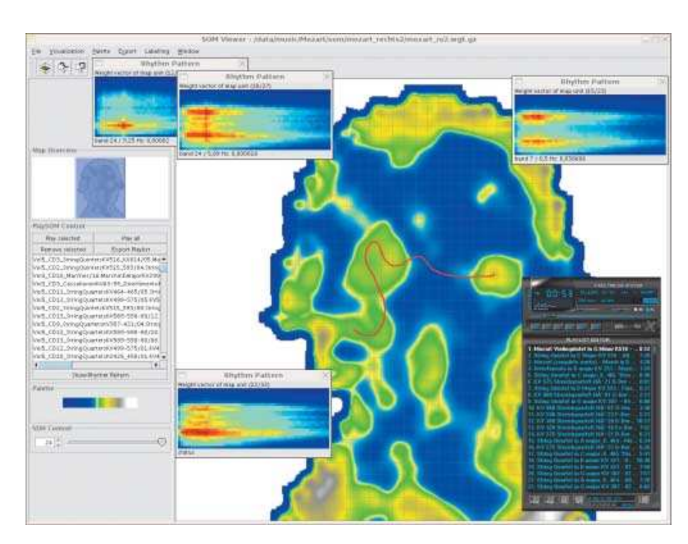
Musikalische Reisen planen

Außer dem Web-Interface gibt es noch PlaySOM sowie PocketSOM, die Variante für PDAs. Beide können noch etwas mehr, und so lassen sich mit diesen Tools ganze Reisen durch Mozarts Welt planen. Mit beschwingter Feder zeichnet man eine Route auf die Karte (siehe Abb. 2) und fertig ist die Playlist, die man sogleich in den Audio Player laden und konsumieren kann.

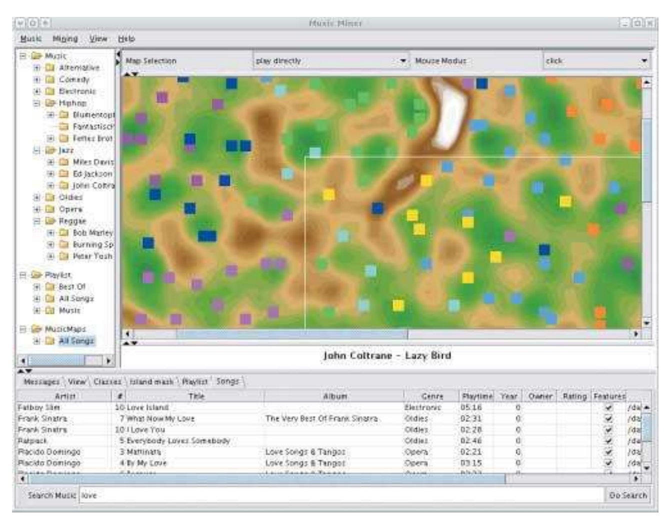
Informatiker fragen sich naturgemäß sofort, was hinter der Bühne vor sich geht und wie der Rechner als vollautomatischer Kartograf diese Landschaft aus Klängen zu zeichnen vermochte. Zunächst wäre da das Konzept der Ähnlichkeit, und es drängt sich die Frage auf, wie sich diese tatsächlich definiert. Die Ähnlichkeit zwischen zwei Stücken zu bestimmen ist nicht trivial, denn wann darf Stück A als ähnlicher zu B gelten als zu C und wann nicht? Für die Berechnung wurden bei der Mozartkarte rein objektive Merkmale herangezogen und keine subjektiven, vom Menschen per Hand gesammelten. Die Analyse der Werke erbrachte zahlreiche Merkmale wie die rhythmischen Muster für 24 Frequenzbänder, statistische Spektraldeskriptoren und Rhythmus-Histogramme aus der Audioinformation. Anschließend erfolgte eine Gewichtung der Merkmale sowie deren Speicherung in einem mehrdimensionalen Vektor.



Die Map of Mozart ordnet seine Werke gemäß klanglicher Ähnlichkeit auf kleinen Inseln an und blendet diese Musiklandschaft über das Gesicht des Künstlers (Abb. 1).



Beherztes Ziehen der Maus über die kleine Inselwelt aus Mozarts Werken genügt, und PlaySOM erstellt eine abspielfertige Playlist aus den ausgewählten Stücken (Abb. 2).



MusicMiner ermöglicht das spielerische Durchwandern der eigenen Klangwelten und klassifiziert die MP3-Sammlung auf den lokalen Festplatten (Abb. 3).

Von da an ist die Ähnlichkeitsanalyse kein Hexenwerk mehr: Ein Merkmalsvektor repräsentiert jedes Werk, und eine Ähnlichkeitsanfrage kommt einer Messung des Abstands beider Vektoren gleich, typischerweise durch die euklidische Distanz oder diverse Korrelationskoeffizienten realisiert.

Der Fluch der Dimensionen

Dies allein erklärt jedoch nicht das Zustandekommen der opulenten Seenlandschaft. Tatsächlich ist die Mozart-Karte im Hinblick auf die automatische Kartografie gar nicht so innovativ wie es scheint. Sie verwendet Verfahren, die schon Anfang der Achtziger konzipiert und bis dato sukzessive verfeinert wurden. Es sind jene eingangs erwähnten Self-Organizing Maps, kurz SOMs.

Eine SOM ist ein visuelles Verfahren mit dem Ziel, einander ähnliche Artefakte, im vorliegenden Fall Musikstücke, räumlich zusammenzufassen und vornehmlich für den Menschen aufzubereiten. Meist dient der zweidimensionale Raum als Projektion. Es handelt sich um ein Clustering-Verfahren, wie es im Data Mining gängig ist. Während herkömmliche Verfahren, wie k-Means (siehe [2]), Expectation Maximization oder die Gattung der dichtebasierten Methoden zwar akkurate Ergebnisse liefern, sind sie für den Menschen in einer Hinsicht leider völlig nutzlos: Er kann die gefundenen Cluster nicht sehen, sondern nur durch statistische Größen erfassen. Clustering findet immer im mehrdimensionalen Merkmalsraum statt und die Zahl der Merkmale der einzelnen Objekte in einem solchen Raum, wie auch der Fall bei den Werken Mozarts, ist in der Regel weit höher als die mageren drei Dimensionen, die sich dem Menschen erschließen. So sind Merkmalsvektoren mit 1000 oder gar mehr Dimensionen keine Ausnahmen, sondern eher die Regel.

Self-Organizing Maps heben im Grunde genau dieses Manko auf: Sie führen ein Clustering der Eingabevektoren durch, reduzieren zeitgleich jedoch die Anzahl der Dimensionen des Merkmalraumes so drastisch, dass das Resultat für den Menschen visuell fassbar wird. Darum sind SOMs über die Grenzen der Wissenschaft und angewandten Forschung hinaus so beliebt. Bilder statt Zahlen ist das Credo.

Musik, das Web und noch mehr

SOMs kommen mittlerweile an allen Ecken und Enden zum Einsatz, die Menge der Publikationen zu diesem Thema hat schon lange die Marke 5000 überschritten. Und gerade in den letzten Jahren lässt sich beobachten, dass die schon vor fast dreißig Jahren entdeckten Karten eine Renaissance erleben.

Thematisch verwandt mit der Mozart-Karte ist MusicMiner (siehe [3]), eine Entwicklung der Universität Marburg. Im Gegensatz zu seinem Pendant der TU Wien zielt dieses Open-Source-Projekt allerdings nicht auf die Klassifikation der Werke Mozarts ab, sondern auf die Kartografierung der eigenen, auf der lokalen Festplatte gespeicherten MP3-Sammlung. Die verwendete Technik heißt ESOM, ein Derivat der SOMs und Kürzel für Emergent Self-Organizing Maps. Die Landschaft ist weniger von Inseln, als vielmehr von Bergketten geprägt (siehe Abb. 3). Auch die Interpretation der Karte ist etwas anders, und so dienen jene erwähnten Gebirgszüge zur Abgrenzung, während sich in einem Tal klangtechnisch ähnliche Titel tummeln. Darum wäre zwischen einem Hip-Hop- und einem Techno-Tal mit Sicherheit eine steile Wand anzutreffen.

Um die MP3-Sammlung in ein hübsches und interaktives Kärtchen zu pressen, muss sich der Anwender vor allem in der Gabe der Geduld üben, denn der Prozess der Merkmalsextraktion aus den Songs geht quälend langsam vonstatten. Bereits die bescheidene Kollektion des Autors aus weniger als 1000 Liedern nahm den Rechner nahezu acht Stunden in Beschlag. Personen mit einer starken Affinität zum Sammeln von MP3s sollten deshalb entweder ordentlich



- Self-Organizing Maps dienen seit den frühen Achtzigern als probates Mittel zur Visualisierung von Daten-Clustern.
- Mit Anwendungen wie der Map of Mozart dringen diese Karten nun verstärkt ins Bewusstsein einer breiteren Öffentlichkeit, vor allem dank der immer ausgefeilteren Darstellungsmethoden.
- Die Intuition der SOMs ist recht simpel, und so können diese ohne größeren Aufwand nachprogrammiert werden.

Zeit mitbringen oder sich die Nutzung des MusicMiner zweimal überlegen.

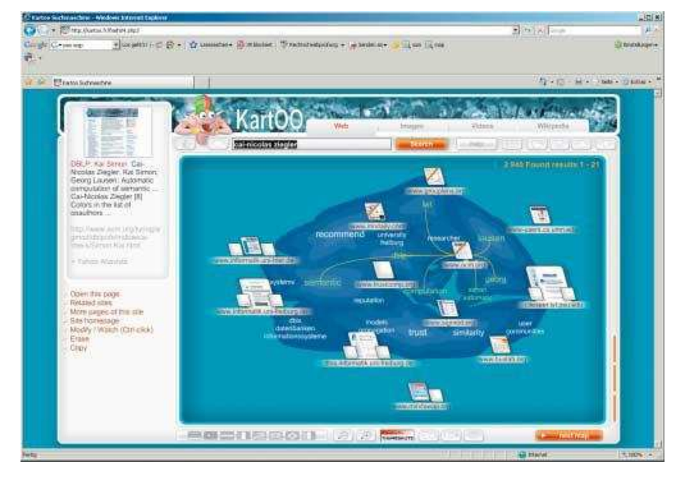
Ein anderes ehrgeiziges Projekt namens WebSOM [4] treibt die Truppe um den Urvater Kohonen selbst voran: das Clustering von großen Dokumentmengen aus dem Internet, darunter die Aufbereitung von etwa einer Million Postings aus 80 Newsgroups. Zwar sind Musik und Text völlig verschiedene Medientypen, dennoch lässt sich das Prinzip der SOMs hier auf nahezu analoge Weise anwenden. Lediglich die Feature-Extraktion ist anders als bei Klangdaten. Bei Text gelten Wörter oder Wortpaare als Merkmale. Dabei besteht ein derartiger Feature-Vektor, der ein einzelnes Dokument repräsentiert, aus ebenso vielen Dimensionen wie unterschiedliche Wörter im Gesamtkorpus auftreten. Der Vektor zählt nur noch die Zahl der Vorkommnisse jener Wörter in einem Dokument. Enthält eins beispielsweise das Wort „Miriam“ dreimal, würde die dazugehörige Komponente des Vektors den Wert 3 zugewiesen bekommen.

WebSOMs Karten erinnern weniger an Inseln, Berge und Täler als vielmehr an eine amorphe und magmatische Substanz. Tatsächlich handelt es sich beim Verfahren um das ursprüngliche, das lediglich auf Durchsatz und Performance getrimmt war: So vermag WebSOM Karten auf einer Datenbasis von bis zu sieben Millionen Dokumenten zu berechnen.

Jenseits des Elfenbeinturms

SOMs finden auch in der außeruniversitären Welt ihre Verwendung. So kommen sie als probates Mittel im Marketing und der webzentrierten Meinungsforschung (siehe [5]) zum Einsatz. Beispielsweise, wenn es um die Analyse und inhaltliche Gruppierung von Nachrichten und Meinungen zu einem bestimmten Unternehmen geht oder um die Auswertung von Kundenfeedback. Eine Beratungsfirma, die sich auf diesen Einsatz von SOMs spezialisiert hat, ist evolve24.

Suchergebnisse zu visualisieren ist ein an Brisanz zunehmendes Thema. Kartoo Technologies, eine französische Firma, hat sich diesem Ziel verschrieben. Im Web ist eine Applikation gleichen Namens zur Schau gestellt, die als Meta-Suchmaschine fungiert und die Resultate einer Suchanfrage grafisch auf Hochglanz poliert (siehe Abb. 5). Zwar gibt Kartoo keine genauen Details zu den Mechanismen, aber die Art der Darstellung lässt nahezu zweifelsfrei auf SOMs schließen. Nebenbei ist das Labelling der geclusterten Daten, die Vergabe passender Namen für dichtere Regionen der Karte, von exzellenter Qualität.



Kartoo leitet eine Anfrage an diverse Suchmaschinen weiter, integriert die Resultate und formt eine mit Schlüsselbegriffen angereicherte Landkarte daraus (Abb. 5).

Karten selbst organisieren

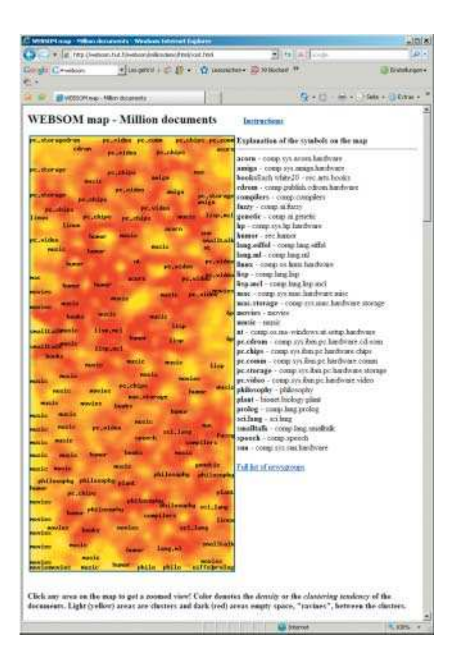
SOMs sind schön anzusehen, nützlich und von der Theorie her nicht übermäßig kompliziert. Im Folgenden soll darum eine Besprechung der Mutter aller Algorithmen rund um SOMs erfolgen. Eine Umsetzung in eigenen Code ist von hier aus ein Leichtes und zudem nur mäßig umfangreich.

Von der Gattung her sind SOMs neuronalen Netze zuzuordnen, gleichzeitig jedoch den Clustering-Verfahren. Sämtliche zu strukturierende Daten, seien es Dokumente, Musikstücke oder andere Medienobjekte, sind als Merkmalsvektoren angenommen. Als weiterer Bestandteil des Versuchsaufbaus kommt ein Gitternetz aus Neuronen hinzu. Meist ist es rechteckig, wie beim MusicMiner oder WebSOM. Doch bestätigen Ausnahmen bekanntlich die Regel, und so besitzt das Neuronennetz bei der Map of Mozart eben keine rechteckige Form, sondern stellt das Konterfei Mozarts dar. Jedes Neuron ist wiederum ein Vektor, und zwar derselben Dimensionalität wie die Eingabedaten.

Zu Beginn ist das Gitternetz wüst und leer. Dies manifestiert sich dadurch, dass jedes Neuron mit zufälligen Werten initialisiert ist. Würde man diese Karte nun visualisieren, sähe man ein Bild, das dem Rauschen eines Fernsehers recht nah käme und bar jeglicher Ordnung und Struktur erschiene.

Täglich grüßt das Murmeltier

Der Algorithmus tritt nun in eine Iterationsschleife ein, die er so lange durchläuft, bis sich die Karte stabilisiert hat und Konvergenzkriterien erfüllt sind. Als Erstes greift sich der Rechner zufällig ein vektorisiertes Eingabedatenobjekt heraus, in der Praxis als Sample bezeichnet. Nun durchläuft er das gesamte Gitternetz und sucht nach dem Neuron, das dem Sample am stärksten ähnelt (siehe Abb. 6). Zu diesem Zweck kommt die zu Beginn erwähnte Ähnlichkeitsmetrik ins Spiel. Dabei hat sich im Hinblick auf die Berechnung von SOMs die euklidische Distanz etabliert, als gangbare Alternative wäre weiterhin die im Information Retrieval häufig anzutreffende Kosinusdistanz denkbar. Letztere misst den Winkel zwischen zwei



Die Gruppe um Kohonen, den Erfinder der Self-Organizing Map, erforscht deren Anwendung auf große Textkorpora, wie hier eine Sammlung aus etwa einer Million News-group Postings (Abb. 4).

Vektoren und nimmt den Kosinus davon (siehe [6]).

Sobald der Gewinner feststeht, findet ein Austausch an Information statt und das Eingabe-Sample färbt sozusagen auf jenes Siegerneuron ab. Im Klartext heißt dies, dass dessen Vektor mit dem des Sample verschmilzt. Wie stark das Neuron die Werte des Sample annimmt, von diesem lernt, hängt von mehreren Parametern ab. Der wichtigste ist ein von der Zeit abhängiger Faktor, der gewährleistet, dass jenes Abfärben mit jeder getätigten Iteration an Intensität verliert. In der Regel handelt es sich hier nicht um eine streng lineare Abnahme der Lernrate, sondern um eine durch eine geglättete Kurve angedeutete.

Den Nachbarn etwas abgeben

Jedoch lernt nicht nur das Siegerneuron selbst vom Eingabe-Sample, sondern außerdem die Neuronen in seiner unmittelbaren Umgebung, seine Nachbarn. Wann ein Neuron als Nachbar gilt, hängt von einer eigenen Funktion ab, die den geografischen Abstand des Siegers zu allen anderen Neuronen im Gitter berechnet und diesen Abstandswert ebenso einer Glättung sowie einer nachfolgenden Normalisierung unterzieht.

Auch die Nachbarschaft bleibt vom Zahn der Zeit nicht verschont und so nimmt mit zunehmender Zahl an Iterationen die Stärke jener nachbarschaftlichen Beziehungen ab. Galt Neuron A in der ersten Schleife noch als eng mit B benachbart, so ist diese Enge nach 100 und mehr Durchläufen nicht mehr derart stark gegeben. Kurz und knackig: Nach der Ermittlung des Siegers und Berechnung der Nachbarschaften liegt für jedes Neuron im Gitternetz ein Wert zwischen 0 und 1 vor, welcher die Nähe zum Gewinner ausdrückt. Je näher das Neuron, desto höher jener Wert. Der Sieger selbst hat dabei einen Wert von 1. Zugleich ist der Distanzwert ein Indikator für die Intensität, mit der das Eingabe-Sample abfärbt.

Auf den Punkt gebracht

Wiederholungen der angeführten Schritte lassen aus dem anfänglich zufälligen Rauschen schließlich ein Artefakt aus Konturen entstehen, aus Verdichtung und Auflockerung im Hinblick auf die Ähnlichkeit räumlich naher Neuronen. Zu klären bleibt nur noch, wie denn nun aus dem Gitternetz eine tatsächliche Karte entsteht. Im einfachen Fall repräsentiert jedes Neuron einen Bildpunkt. In diesem Fall ist ihm im Folgeschritt eine Farbe zuzuordnen, wobei die Farbskala als Verlauf angenommen sei (siehe Abb. 4) und sich die Bestimmung somit auf die Ermittlung eines Indexwerts in dieser Skala beschränkt. Intuitiv entspricht dieser Indexwert der Ähnlichkeit des betrachteten Neurons zu seinen jeweiligen Nachbarn, je höher diese Ähnlichkeit, desto höher der Indexwert. Gewöhnlich werden starke Ähnlichkeiten zur Umgebung durch leuchtintensive, helle Farben ausgedrückt. Oder eben, in den Darstellungsweisen, die mit Höheninformation arbeiten, durch Bergkuppen. Streng kohärente Cluster artikulieren sich folglich durch helle Flecken oder Himmelsnähe.

Eine ausführliche Beschreibung der Technik zur Berechnung von SOMs enthält [4]. Darin sind auch Optimierungsverfahren zu finden, vor allem im Hinblick auf die Rechenperformance und Ansätze zur Verbesserung der Kartenqualität, beispielsweise durch die Reduktion der Dimensionalität der Eingabe-Samples.

Für jedes Eingabe-Sample wird das Neuron im Gitter bestimmt, das diesem am nächsten kommt. Sodann lernen der Gewinner und dessen Nachbarschaft vom Sample und werden hierdurch diesem ähnlicher (Abb. 6).

Fazit

Neben den SOMs ist die Gruppe der dedizierten Algorithmen zur Visualisierung von Clustern recht überschaubar. Erwähnenswert in diesem Kontext wäre noch die als Multi-dimensional Scaling bekannte Methode [6]. Allerdings kann diese in puncto Popularität den SOMs bei Weitem nicht das Wasser reichen. SOMs sind der Stand der Technik und finden auch in großen Data-Mining-Plattformen wie der von SAS ihren Niederschlag.

Und sie sind mehr als bloßer Tand, mehr als ein durchdachter Marketinggag im Fahrwasser der Feierlichkeiten berühmter Persönlichkeiten. Menschen wollen sehen, Daten und Zusammenhänge erkennen. SOMs ermöglichen es ihnen; sie sind das Endoskop der Informationswelt. (hb)

DR. CAI ZIEGLER

arbeitet als Consultant bei der Siemens AG, Corporate Research & Technologies. Dort beschäftigt er sich mit Self-Organizing Maps zur Visualisierung der Siemens-internen Blogosphäre.

Literatur

[1] Geoskop; Informatik: Mozart à la carte; Geo Magazin 06/06, S. 187

[2] Jiawei Han, Micheline Kamber; Data Mining: Concepts and Techniques; Morgan Kaufmann Publishers, 2001

[3] Sven Hansen; Musik für Ihren Geschmack: Vorschlagssysteme für Musik im Einsatz; c't 04/2006, S. 194

[4] Krista Lagus et al.; Mining Massive Document Collections by the WEBSOM Method; Information Sciences, 2004; 163 (1-3), S. 135

[5] Cai Ziegler; Stummer Wächter: Reputation Intelligence und Sentiment Detection; *iX* 4/2006, S. 116

[6] Soumen Chakrabarti; Mining the Web; Morgan Kaufmann Publishers, 2003

Onlinequellen

[a]	Map of Mozart	www.ifs.tuwien.ac.at/mir/mozart/
[b]	MusicMiner	musicminer.sourceforge.net/
[c]	Meta-Suchmaschine Kartoo	www.kartoo.com/



Langzeitarchivierung mit Evidence Record Syntax

Hält sicher

Tobias Gondrom

Seit Januar 2008 empfiehlt das Bundesamt für Sicherheit in der Informationstechnik eine Mindestschlüssellänge von 2048 Bit für die Signaturverfahren RSA und DSA. Der neue IETF-Standard Evidence Record Syntax hilft, die Beweiskraft elektronischer Dokumente und Signaturen zu sichern.

Eine der maßgeblichen Anforderungen der Langzeitarchivierung ist der Schutz vor unberechtigten Eingriffen. Um unabsehbare Rechtsrisiken mit elektronischen Dokumenten abzufangen, müssen diese im Zeitverlauf – dies können Jahre oder wie im Falle von Patientenakten auch Jahrzehnte sein – nachvollziehbar und beweisbar vor Änderungen geschützt werden. Jede Manipulation, etwa aufgrund technischer Fehler oder absichtlicher Verfälschungen, muss sich sicher erkennen lassen.

Daher baut der Gesetzgeber auf die elektronische Signatur, die, je nach Stufe, sogar die Beweiskraft einer Unterschrift genießt und in der Regel eine Public-Key-Infrastruktur (PKI) voraussetzt. Die Beweiskraft elektronischer Signaturen und Daten nimmt jedoch mit der Zeit ab – ein entscheidender Unterschied zur manuellen Unterschrift. Die Bundesnetzagentur veröffentlicht im Bundesdatenanzeiger die Zeiträume, in denen die für elektronische Signaturen verwendeten Algorithmen als sicher gelten. Wer nach dem Ablauf dieser Sicherheitseignung noch auf die Echtheit der alten Signaturen, ihre Beweiskraft und den Anscheinsbeweis zählen will, muss sie rechtzeitig mit stärkeren Signaturen erneuern (§ 17 SigV). Besonders betrifft das Dokumente, die langfristig archiviert werden müssen und über den gesamten Zeitraum ihre volle gesetzliche Beweiskraft behalten sollen.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) sieht die noch häufig verwendeten Signaturen nach dem RSA- und DSA-Verfahren mit einer Schlüssellänge von 1024 Bit seit Anfang 2008 nicht mehr als vertrauenswürdig an. Unternehmen müssen viel Zeit und Geld einplanen, wenn sie gezwungen sind, die Signaturen bei einer großen Anzahl von Dokumenten zu erneuern.

Diese ökonomischen Aspekte haben – neben dem geforderten maximalen Sicherheitsniveau und der weltweiten Austauschbarkeit der Beweisdaten – die Arbeit der IETF-Arbeitsgruppe LTANS bestimmt. IETF steht für Internet Engineering Task Force, LTANS für Long-Term Archive and Notary Services. Sie wollte Mechanismen entwickeln, die mit dem Knacken von Verschlüsselungsalgorithmen, Anforderungen nach größeren Schlüssellängen oder der Beschädigung privater Schlüssel des Unterzeichners umgehen können. Tritt nur ein solcher Vorfall ein, lässt sich ohne erneuerte Signatur weder die Echtheit des Dokuments noch die Identität des Unterzeichners garantieren.

Dokumente für die Ewigkeit

Ergebnis der Arbeit: der im August 2007 von der IETF verabschiedete international gültige Standard ERS (Evidence Record Syntax) oder RFC 4998. Er orientiert sich an den Ergebnissen des ArchiSig-Projekts, das ein großes interdisziplinäres Konsortium unter der Förderung des Bundesministeriums für Wirtschaft und Arbeit durchgeführt hat. ArchiSig beschäftigte sich mit den Erfordernissen einer rechtssicheren Langzeitarchivierung. ERS definiert im Detail, wie man Signaturen für große Dokumentenmengen automatisch und wiederholt erneuert. Darüber hinaus legt der Standard die Datenformate fest, in denen sich die Beweisdaten über einen unbegrenzten Zeitraum bereitstellen und rechtssicher austauschen lassen. Teile aus den Dokumentenbeständen können dabei gelöscht werden, ohne dass dies die Beweiskraft der übrigen Teile beeinträchtigt.

Die Idee, die ERS umsetzt, besteht in dem erneuten Sig-

iX-TRACT

- Elektronische Signaturen und Zeitstempel an Dokumenten können durch Ereignisse wie dem Knacken von Schlüsseln ihre Glaubwürdigkeit und rechtliche Beweiskraft verlieren.
- Das Erneuern von Signaturen und Zeitstempeln an aufbewahrungspflichtigen Dokumenten stellt deren Integrität für einen bestimmten Zeitraum sicher.
- Der internationale Standard Evidence Record Syntax hilft Unternehmen beim Aktualisieren der Schutzmechanismen für wichtige Dokumente. Um ihn herum soll ein Framework aus flankierenden Standards entstehen.

nieren mit neuen und stärkeren Algorithmen, sodass im Zeitverlauf gleichsam verschiedene Schutzschichten um die Dokumente entstehen. Um den damit verbundenen Aufwand klein zu halten, kombiniert man Hash-Bäume (nach Merkle) mit Zeitstempeln. Dadurch benötigt nicht jedes einzelne Dokument einen eigenen Zeitstempel. Die Echtheit der Dokumente lässt sich verifizieren, ohne dass man dabei von den anderen Dokumenten in demselben Hash-Baum wissen muss. Der Standard erlaubt eine unbegrenzte Anzahl an Signaturerneuerungen.

Als Vertrauensanker dienen ERS die kryptografischen Algorithmen und ein akkreditierter Zeitstempel. Damit hängt das Verfahren weder von der Vertrauenswürdigkeit eines Storage-Anbieters, einer Behörde noch einer Einrichtung ab, die signierte Dokumente treuhänderisch oder unter notarieller Aufsicht aufbewahrt. Jedes Unternehmen kann seine Dokumente selbst rechtssicher aufbewahren und deren Integrität gegenüber Dritten unabhängig vom eigenen System beweisen. Schließlich garantieren das Standarddatenformat und das Protokoll ein reibungsloses Zusammenspiel sowie die unabhängige Verifizierung mit unterschiedlichen Applikationen.

Zeitstempel im Kompaktformat

Eine der Grundlagen des ERS-Konzepts bilden die sogenannten Archivzeitstempel, die sich anders als einfache Zeitstempel auf viele Datenobjekte beziehen. Ein Archivzeitstempel kombiniert einen Hash-Baum mit einem Zeitstempel, der die Integrität des Hash-Baumes sichert. Bildlich gesprochen ähnelt dies einem Sack, dessen Siegel seine Vertrauenswürdigkeit und die seines Inhalt garantiert. Die einzelnen Dokumente sind die Blätter des Hash-Baumes. Ein Zeitstempel ist nur für den Ursprungswert an der Spitze des Baumes nötig. Gemäß ERS lässt sich der Baum auf die für den Integritätsbeweis eines einzelnen Dokumentes relevanten Werte reduzieren und kommt so mit einem sehr kleinen Datensatz aus. Diese Wertemengen plus Zeitstempel ergeben den Archivzeitstempel (Abb. 1, oberer Teil).

Das genaue Verfahren: Ein Hash-Baum fasst Gruppen von Hash-Werten auf einer Ebene zusammen. Daraus wird ein neuer Hash-Wert berechnet. Dadurch kann man einen großen Teil des Baumes, der nicht direkt für die Berechnung eines bestimmten Pfad notwendig ist, weglassen und die Datenmenge des Archivzeitstempels auf eine kleine Untermenge reduzieren. Wichtig ist, dass sich die gesamte Kette vom Dokument bis zum obersten Knoten des Baumes, dem Zeitstempel, mathematisch eindeutig zurückverfolgen lässt. Informationen aus Verzweigungen, die sich nicht direkt auf die Berechnung der Werte der jeweils höheren Ebene beziehen, bleiben unberücksichtigt. Die letzte Stelle der entstehenden Datenmenge im Zeitstempel belegt der Hash-Wert der Ursprungsverzweigung.

Um einen Zeitstempel für ein bestimmtes Datenobjekt zu verifizieren, reicht es aus, den Weg vom Hash-Wert des Dokuments bis zum Ursprungswert zurückzuverfolgen. Die Kette der einzelnen Werte bis zum Ursprung lässt sich errechnen und mit dem Originalzeitstempel vergleichen (Abb. 1). Kleines Beispiel: Wenn der Pfad für die Prüfung der Signatur eines Datenobjekts

$d1 \rightarrow h1 \rightarrow h5 \rightarrow t$

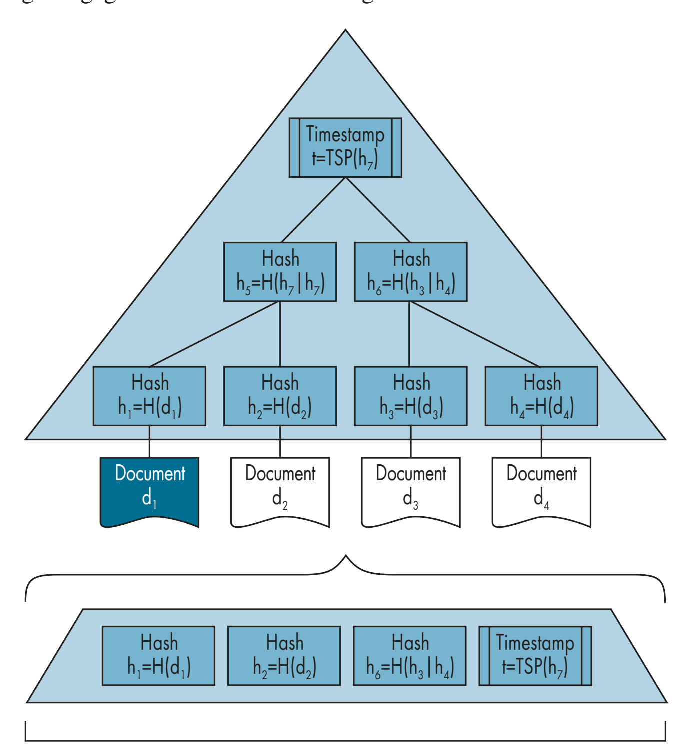
lautet, muss die mathematische Probe diese Bedingung erfüllen:

$H(H(h_1|h_2)|h_6) = H(h_5|h_6) \in TSP.$

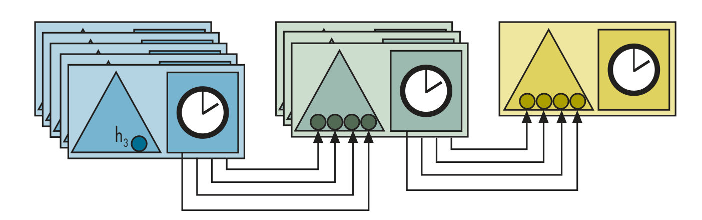
Dokumente, die bei einem Unternehmen oder einem Speichersystem eintreffen, können anfangs durch verschiedene Algorithmen und somit für unterschiedlich lange Zeiträume gesichert sein. Das könnte dazu führen, dass die Verantwortlichen einige Dokumente bereits nach Wochen erneuern müssen, andere hingegen erst nach Jahren. Da ERS diesen Vorgang von der Anzahl der Dokumente weitgehend entkoppelt, wäre es klug, alle bei Eingang auf ein gleichmäßig hohes Sicherheitsniveau zu heben. Dazu muss man die Dokumente zunächst mit einem initialen Archivzeitstempel versehen. Damit entfällt die Notwendigkeit, die verschiedenen Formate und Algorithmen in jedem einzelnen Datenobjekt zu analysieren. Vielmehr kann das System sich auf die bekannten Sicherheitsparameter der initial verwendeten Zeitstempel verlassen. Auf der Basis dieses Sicherheitsankers kann ein System entscheiden, die Daten erneut zu signieren, wann immer das Sicherheitsniveau der verwendeten Algorithmen nachlässt.

Im Alter verfällt der Schutz

Prinzipiell muss ein System für rechtssichere Langzeitarchivierung in der Lage sein, sowohl die Signatur- und Zeitstempel-Algorithmen als auch die im Hash-Baum verwendeten Algorithmen erneuern zu können. Zeitstempel verlieren ihr Sicherheitsniveau, wenn die verwendeten Algorithmen (etwa Public-Key) oder die Schlüssellängen nicht mehr zuverlässig sind. Die Sicherheitseigenschaften des Hash-Baumes können ebenfalls veralten und dann beispielsweise die Be-



Hash-Baum und seine komprimierte Variante (unten): Wer einen Zeitstempel für ein bestimmtes Objekt verifizieren will, muss lediglich den Weg vom Hash-Wert des Dokuments bis zum Ursprungswert zurückverfolgen (Abb. 1).



Verknüpfte Hash-Bäume: Das wiederholte Erneuern des Zeitstempels erhält den Beweiswert aller Dokumente (Abb. 2).

dingungen für Widerspruchsfreiheit und Unumkehrbarkeit nicht mehr erfüllen.

Beide Szenarien erfordern einen erneuerten Schutz. Ein aktualisierter Zeitstempel lässt sich schnell und effizient innerhalb weniger Sekunden für beliebig viele Dokumente gestalten. Da er den Hash-Wert enthält, der den gesamten Baum repräsentiert, ist es nicht nötig, die damit geschützten Dokumente aufzurufen und für sie neue Hash-Werte zu errechnen. Vielmehr wird einfach der oberste auslaufende Zeitstempel in einen neuen Hash-Baum eingetragen und durch einen stärkeren Zeitstempel gesichert – so als ob man einen versiegelten Dokumentensack in einen größeren Behälter packen und diesen mit einem neuen starken Siegel versehen würde. Auf diese Weise bleibt der Beweiswert aller Dokumente bestehen (Abb. 2).

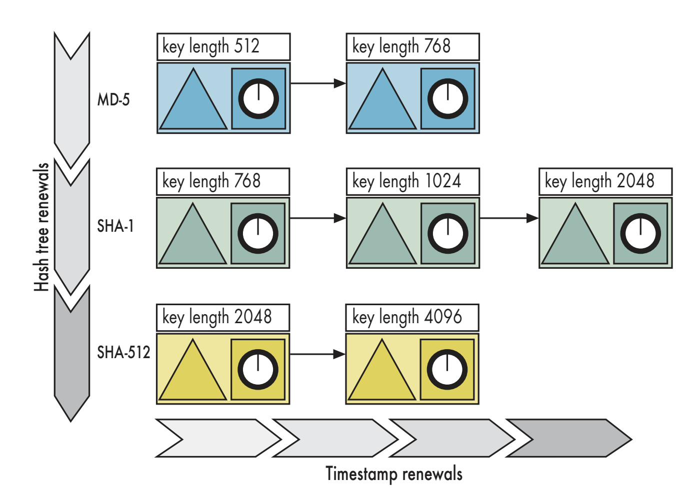
Die Erneuerung der Hash-Algorithmen ist ungleich aufwendiger, findet allerdings auch viel seltener statt. Oft wird sie gar nicht notwendig sein, manchmal nur alle 20 Jahre. Wenn der Baum an Sicherheit verliert, muss das System für sämtliche Dokumente neue Werte auf der Basis eines aktuellen Algorithmus berechnen. Die neuen Werte werden gemeinsam mit den bereits bestehenden Beweisdaten in neue Hash-Bäume eingetragen. Natürlich müssen diese nur einen einzigen Zeitstempel an der Spitze tragen (Abb. 3).

Die Hash-Baum-Erneuerung ist aufwendiger als die eines Zeitstempels. Daher empfiehlt es sich, redundante Hash-Bäume zu verwenden (Abb. 3).

Trotz der effizienten Gestaltung kann der Lesezugriff auf Millionen oder gar Milliarden Dokumente bei der Berechnung neuer Hash-Werte längere Zeit dauern und somit teuer sein. Um dem zu begegnen, sieht ERS den Einsatz mehrerer paralleler Hash-Bäume vor, die auf unterschiedlichen Algorithmen basieren. Unterschreitet einer der Bäume das geforderte Sicherheitsniveau, ist das Dokument immer noch durch mindestens einen weiteren geschützt.

ERS definiert Datenstrukturen in der Beschreibungssprache ASN.1 (Abstract Syntax Notation One). Eine XML-Version befindet sich in Vorbereitung. Die Datenstrukturen speisen sich aus drei Quellen: dem Archivzeitstempel sowie erneuerten Zeitstempeln und Hash-Bäumen. Im Ergebnis entsteht eine Liste mit Archivzeitstempeln, von denen jeder einzelne auf den jeweils nächsten in chronologischer Reihenfolge verweist. So bildet sich eine vollständige Beweiskette für die gesamte Aufbewahrungszeit eines Dokuments, die sich von unabhängigen Dritten verifizieren lässt (Abb. 4).

Die Prüfung der elektronischen Signaturen erfolgt in zwei Schritten. Zunächst wird der Zeitpunkt bestimmt, bis zu dem sie gültig sind. Auf Basis dieses Referenznachweises (Evidence Record) lässt sich dann beweisen, dass das Dokument und alle verwendeten Signaturen vor ihrem Verfallsdatum existierten und sie seitdem niemand verändert hat. Um den Beweiswert bestehender Signaturen im Dokumentenbestand zu erhalten, müssen die Archivzeitstempel höchsten Sicherheitsstandards genügen. Dazu empfiehlt sich der Einsatz der sichersten Public-Key- und Hash-Algorithmen sowie Zeitstempeln von einem akkreditierten Aussteller – Qualitäten, die der anspruchsvollsten vom Gesetzgeber definierten Signaturstufe entsprechen.



Algorithmuserneuerung im Zeitverlauf: Es entsteht eine lückenlose Beweiskette für die gesamte Aufbewahrungszeit eines Dokuments (Abb. 4).

Ergänzende Standards in Sicht

Die Verabschiedung des ERS-Standards bedeutet nicht das Ende der IETF-Arbeitsgruppe LTANS. Sie arbeitet an weiteren Standards, etwa einem Protokoll für den Zugriff auf Dienste zur Langzeitarchivierung, einer Sicherheits-Policy für die automatische Auswertung von Archiven sowie an Verifikationssystemen und Best Practices für den Umgang mit Algorithmen und Verifizierungsdaten. Diese Spezifikationen sollen ERS flankieren und im Zusammenspiel neue Möglichkeiten eröffnen. Der ersten großen Aufgabe in der Geschichte elektronischer Signaturen allerdings tritt ERS allein entgegen. Dieser Standard muss die Verantwortlichen in die Lage versetzen, die anstehenden Neusignierungen mit längeren Schlüsseln wirtschaftlich und zuverlässig durchzuführen. (jd)

TOBIAS GONDROM

leitet das Security Team bei Open Text. Zudem ist er Vorsitzender der IETF-Arbeitsgruppe LTANS.

Onlinequellen

Internet Engineering Task Force (IETF)	www.ietf.org
Algorithmenkatalog der Bundesnetzagentur	www.bundesnetzagentur.de/enid/924678f43de0c67d2a23e8a83f821c7b,0/Veroeffentlichungen/Algorithmen_sw.html
Algorithmenkatalog des BSI zur Sicherheitseignung	www.bsi.bund.de/esig/kryptoalg.htm
IETF LTANS-Arbeitsgruppe	www.ietf.org/html.charters/ltans-charter.html
ERS Standard RFC-4998	www.ietf.org/rfc/rfc4998.txt
Leitfaden zur Aufbewahrung elektronisch signierter Dokumente	www.bmwi.de/BMWi/Redaktion/PDF/Publikationen/Dokumentationen/doku-564,property=pdf,bereich=bmwi,sprache=de,rwb=true.pdf



Sicherheit in VMwares Infrastructure 3

Riegel vorgeschoben

Christoph Puppe

VMware ist mit Infrastructure 3 führend in x86er-Server-Umgebungen. Da jede Software Angreifer anlocken kann, sollte man beim Einrichten der Server besonders sorgfältig zu Werke gehen und die Schwachstellen schützen.

Virtualisierung erfreut sich vor allem im Serverbereich zunehmender Beliebtheit, was sicherlich mit an der gestiegenen Leistungsfähigkeit und den großen Speichervolumina heutiger Systeme liegt. Doch gerade, wenn es um zentrale Dienste der IT in Unternehmen geht, sind wirksame Schutzmaßnahmen gefragt. Dabei gibt es einige Unterschiede zwischen physischen und virtuellen Servern.

In einer virtuellen Umgebung legen die physischen Hosts und deren Verwaltungsdienste das Fundament für das Sicherheitskonzept. In „VMwares Infrastructure 3“ (VI3) [1] stehen vier Komponenten im Mittelpunkt: der ESX Server, die Datenbank für die Konfigurationseinstellungen, das Managementmodul „Virtual Center“ (VC) sowie der Arbeitsplatz mit dem Verwaltungs-Client. Das Herzstück, der VMkernel, muss vor allem gegen Angriffe geschützt sein. Um die Sicherheit seiner Virtualisierungslösung unter Beweis zu stellen, hat VMware nach eigenen Aussagen einen Sourcecode Audit unternommen und mit positiven Zitaten der Prüfer geworben.

Ausschlaggebender sind die international gültigen „Evaluation Assurance Level“ (EAL – siehe Onlinequellen [a]). Die vorige Version (ESX 2.5, VC 1.2.0) war für EAL 2 zertifiziert, die aktuelle (ESX 3.01 und VC 2.0.1) ist derzeit für EAL4+ in Vorbereitung. Es gibt laut Definition sieben Stufen. Sie sind jedoch kein Maßstab für die Sicherheit, sondern beschreiben ausschließlich die Ebene, auf der ein System im Test die Anforderungen seines „Protection Profile“ (PP) [b] erfüllt hat. PP folgt dem Evaluierungsprozess der Common Criteria [c].

Eine deutlichere Sprache als die Zertifizierungen und Ausführungen in den Whitepapers des Herstellers sprechen Veröffentlichungen über die Verwundbarkeit der Komponenten. Darunter ist bisher nur eine zu finden, die es einem Angreifer von einer virtuellen Maschine (VM) aus erlaubt hätte anzugreifen [d]. Allerdings nur unter der Bedingung, dass eine saubere Trennung der VMs untereinander und von der Infrastruktur stattgefunden hat. Und von den bedrohlichen Rootkits [2] gab es bis dato nur Laborversionen.

Architektur der VI3: Linux als Pförtner

Das eigentliche Arbeitspferd, der ESX Server – im Folgenden einfach als ESX bezeichnet – startet mit einem angepassten Linux von Red Hat, das es als Boot-Loader für den VMkernel nutzt. ESX läuft nicht auf einem Linux-Kernel, sondern enthält einen eigenen, der als Erstes das „Console Operating System“ (COS) bootet. Es bietet eine Shell, diverse CLI-Befehle, die Daemons zur Verwaltung (*authd*, *hostd*) und eine Weboberfläche auf Basis von Apache sowie Tomcat. Die Authentifizierung beim COS erfolgt über die von Linux bekannten Mechanismen samt der Anbindung an ein Active Directory per PAM.

Der Administrator nutzt hauptsächlich den VI-Client, eine Windows-Anwendung, die er auf seinem Arbeitsplatz installieren muss. Sie erlaubt die Konfiguration fast aller Funktionen der VI3. Der VI-Client verbindet sich per SSL entweder direkt mit ESX oder mit einem Management-Server, dem Virtual Center (VC).

VC hat keine Benutzeroberfläche auf dem Server, auf dem es installiert ist, sondern stellt nur eine Art Proxy zwischen den VI-Clients und den ESX Servern dar. Die Einstellungen sichert das VC entweder in eine lokale „Microsoft SQL Server Desktop Engine“ (MSDE) oder in eine vollwertige Datenbank.

Die Authentifizierung erfolgt über die lokale Benutzerliste oder, sofern verfügbar, das Active Directory. In allen Fällen, in denen in der VI3 mehr als ein ESX notwendig ist, gilt VC als unabdingbare Voraussetzung: etwa für VMotion (Migration), High Availability (Hochverfügbarkeit), Distributed Resource Scheduler und Consolidated Backup. VC bietet nicht nur den Vorteil der gemeinsamen Administrierbarkeit von ESX-Farmen, sondern erlaubt die zentrale Verwaltung von Rollen und Rechten der einzelnen Administratoren, die für unterschiedliche VMs, ESX-Farmen und das VC zuständig sind.

Hinzu kommt der Lizenzserver, der oft auf der gleichen Maschine läuft wie das VC. Da es für alle einmal lizenzierten Optionen eine Spanne von zwei Wochen gibt, in der er nicht erreichbar sein darf und auf ihm keine sicherheitskritischen Daten gespeichert sind, bleibt er in diesem Artikel außen vor.

Eine wichtige Rolle spielt die Farm, eine Gruppe von ESX Servern in einer VI, die eine bestimmte Aufgabe haben oder zu einer Abteilung oder einem Kunden gehören. Innerhalb einer Farm kann es durchaus produktive Systeme wie Test- und Entwicklungsumgebungen geben. In einer VI sind die Server in der Regel an ein Storage Attached Network (SAN) angeschlossen, das über Logical Unit Numbers (LUNs) Speicherbereiche bereitstellt. Die Größe einer Farm schränken drei Faktoren ein: die Zahl der Server, die gleichzeitig auf eine LUN zugreifen, wie viel Rechner dort gespeichert sind und der gewünschten Durchsatz im SAN. Große VI-Umgebungen können über mehrere Farmen verteilt sein.

Trennung vom Netz der Netze

Alle Komponenten einer VI benötigen ein gemeinsames Verwaltungsnetz, über das die Steuerung und der Datenaustausch stattfinden kann. Um zu verhindern, dass eine VM die Kommunikation stört oder ein Angreifer, der sie übernommen hat, die Komponenten der VI angreift, muss das Verwaltungsnetz von den produktiven Netzen der VMs getrennt sein. Zudem sollte es keine Verbindungen zu anderen internen Netzen im Unternehmen geben. Die Trennung kann physikalisch mit separaten Switches oder virtuell mit einem VLAN geschehen. Das COS sollte nicht die gleiche Netzwerkkarte nutzen wie die VMs. Gleiches gilt gegebenenfalls für VMotion und Speichernetze, die etwa iSCSI nutzen. Welches Level infrage kommt, hängt vom angestrebten Sicherheitsniveau und den zu rechtfertigenden Kosten ab. Datenbankserver und Lizenzserver brauchen nur einen Zugang zum VI-Netz und sollten darauf beschränkt bleiben.

Da die Arbeitsplätze der Administratoren oft im Intranet angeschlossen sind, empfiehlt es sich, VC mit zwei Netzwerkkarten auszustatten: eine für die Kommunikation nach innen mit der VI und eine für den Kontakt nach draußen zu den VI-Clients auf den Arbeitsplätzen der Administratoren. Dort kann das VC an das Active Directory angebunden sein, das die Authentifizierung regelt. Bei besonderen Anforderungen an die Sicherheit kann man das VC vollständig hinter eine Firewall verbannen, die eine Trennwand zwischen dem Intranet und dem produktiven Netz der VI-Komponenten aufbaut.

Nicht aus den Augen verlieren sollte man beim Abschotten, einen Weg für die Übertragung von (VMware-) Images (*vmdk*-Dateien) und den Zugang zum ESX per *ssh* zu schaffen. Außerdem sind die Optionen der Physical-2-Virtual-Migration (P2V) eingeschränkt, wenn die zu migrierende Maschine nicht über den Port 903 mit einem ESX kommunizieren kann. Wie der Zugang aussehen sollte, hängt von der Umgebung ab. Bewährt hat sich der Transport von Dateien per *scp* von den Clients der Administratoren aus, weil es über den SSH-Port des ESX geht, sodass für beide Funktionen nur ein Port für die einzelnen IPs des Intranet offen sein muss.

Per Port Forwarding über SSH sind die erweiterten Funktionen auf Port 903 für eine direkte Systemmigration auf einen ESX Server erreichbar. Wichtig ist es, dass der beim Einrichten des ESX Server angelegte Benutzer „Root“ sich nicht über *ssh* anmelden darf. Jeder Administrator, der das COS nutzen und Migrationen durchführen soll, muss als Benutzer im ESX existieren.

Es gibt drei Anwendergruppen: Nutzer und Administratoren der VMs sowie die Administratoren der VI. Erstere benötigen keinerlei Rechte auf den Komponenten der VI und sollten dazu keinen Zugang haben. Innerhalb der Gruppe der VI-Administratoren kann es wiederum feine Unterschiede geben, je nachdem, welche Person welche Rolle erfüllt und welche Rechte damit verbunden sind. Für alle Farmen, eine Farm, einen ESX oder nur eine VM können Benutzer das Recht erhalten, neue Server aufzunehmen, VMs hinzuzufügen, deren Einstellungen zu ändern, sie zu rebooten oder die Konsole der VM aufzurufen.

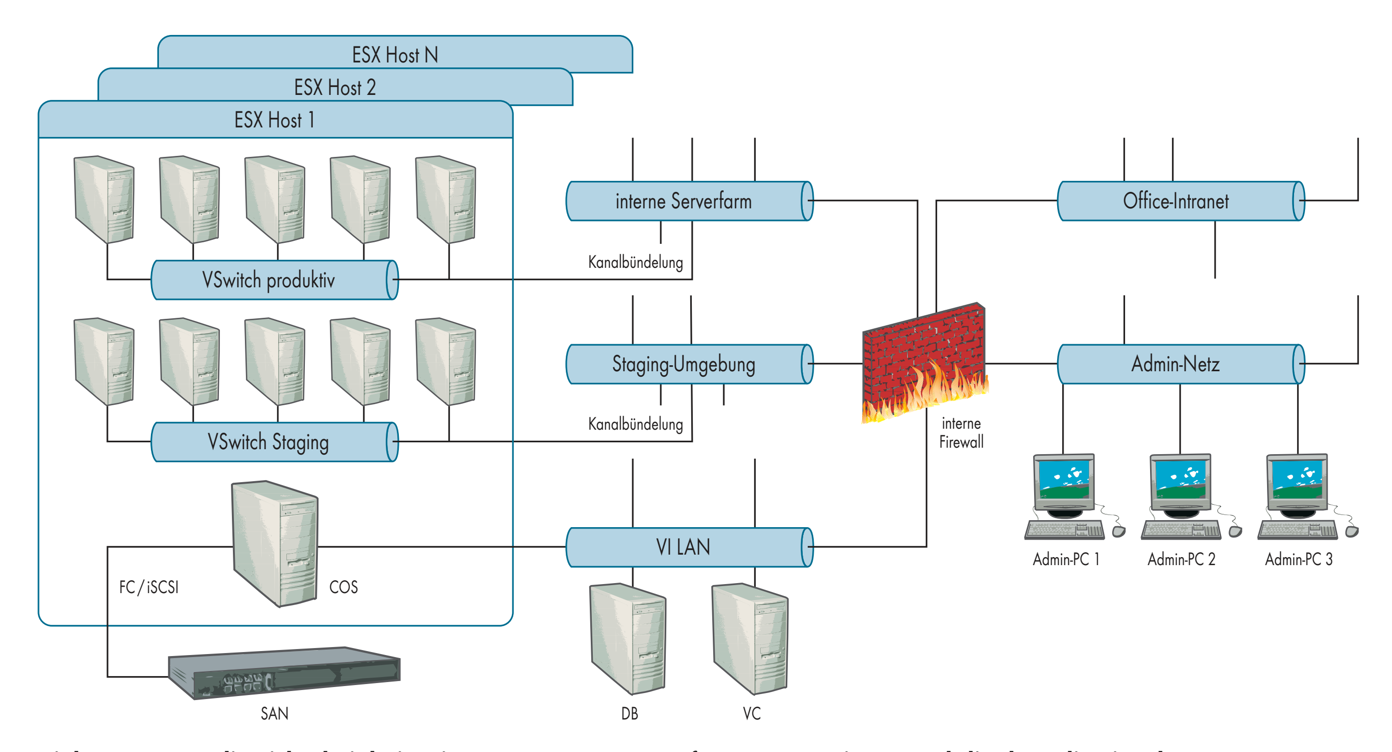
Einmalige Admin-Aufgabe

Der erste einzurichtende User jedes neuen ESX heißt ROOT. Er hat nur einmal die Aufgabe, den Server in die Verwaltung des VC aufzunehmen. Später gibt es im ESX nur noch die Administratoren mit lokaler Zuständigkeit, zu denen die Live-Migration ohne den Umweg über Dateien oder VC gehören kann, und diejenigen mit Rechten zur Übertragung von Dateien, die Accounts auf dem ESX benötigen. Im VC gibt es ebenfalls einen Superuser, der über alle Rechte verfügt und Rechte vergeben darf. Ohne AD ist es immer der lokale Administrator Account. Empfehlenswert ist es, nicht die Admins der Domänen für die Rolle einzutragen, da sie in der Regel nur Rechte auf den Windows-VM benötigen.

In einer überschaubaren Umgebung existiert üblicherweise eine Gruppe von Administratoren, die – bis auf die Rechtevergabe und die VC-Verwaltung – alle übrigen Freiheiten einschließlich des Zugangs zum COS haben. Für eine weitere Untergliederung ist es sinnvoll, die

iX-TRACT

- Die Sicherheit der gesamten virtuellen Infrastruktur (VI) von VMware fußt auf der Zuverlässigkeit der Hardwareplattform.
- Entscheidend ist ein Konzept, das eine saubere Trennung des Verwaltungsnetzes von den produktiven Netzen und von der übrigen Infrastruktur im Unternehmen festlegt.
- Einige Komponenten der VI bedürfen besonders sorgfältiger Prüfung: neben den ESX Servern vor allem das Virtual Center und die Konfigurationsdatenbank.
- Virtuelle Maschinen mit unterschiedlichen Sicherheitsanforderungen sollten nicht im selben virtuellen Netz laufen.



Viele Wege: Für die Sicherheit beim Einsatz von VMwares Infrastructure 3 ist es unabdingbar, die einzelnen Netze voneinander zu trennen, da es sonst zu Übergriffen kommen kann (Abb. 1).

Gruppe klein zu halten und eine weitere Gruppe an Administratoren einzurichten, die nur VMs hinzufügen und verwalten können, aber keine Rechte haben, die Farmen selbst zu verwalten oder auf das COS zuzugreifen. Das Konzept ermöglicht zudem die Mandantentrennung, bei der ein Anbieter von VI-Lösungen seinen Kunden die vollen Rechte auf ihre VMs gibt, aber gleichzeitig die Kontrolle über die VI behält.

Härtung der Komponenten

Ein kritischer Punkt taucht bei der Authentifizierung der VI-Komponenten untereinander auf. Beim Einrichten legt die Prozedur selbst signierte Zertifikate an, die der Administrator bei der ersten Nutzung akzeptieren muss. Wer Hand anlegen möchte, kann die Zertifikate durch selbst erstellte und CA-signierte ersetzen, sollte das aber bereits während der Installation erledigen. Leider gilt dies nur für die Server, eine Authentifizierung des Clients durch den Server per Zertifikat ist nicht vorgesehen.

Jede einzelne Komponente braucht eigene Methoden zur Härtung. Beim ESX Server ist nur wenig zu tun, solange niemand die grundlegende Default-Einstellung *security=high* verändert. Sie stellt sicher, dass der Zugang zum ESX Server nur über stark verschlüsselte Protokolle führt und eine lokale Firewall alle ausgehenden wie eingehenden Verbindungen blockiert, außer *ssh*, *https* und der über den VMware-eigenen Administrationsport 902. Auf dem COS des ESX sollte keiner weitere Software installieren, höchstens zur Überwachung des Betriebs durch Agenten darf es Ausnahmen geben. Schutzsoftware wie Virenscanner oder Ähnliches gehört auf die VMs und haben im COS nichts zu suchen. Und obwohl es sich beim Console Operating System um ein abgespecktes Linux handelt, dürfen niemals die Patches von Red Hat zum Einsatz kommen, nur die von VMware herausgegebenen enthalten die Anpassungen für das COS. Mit der jüngst erschienenen Version 3.5 verbessert sich die Lage: der neue Service „VI Update Manager“ für die Verwaltung der Patches bedient jetzt ESX und COS.

Eine denkbare Lücke, über die jemand von einer VM aus den Wirt beeinflussen könnte, öffnen die Logfiles, die VMwares Tools auf der VM und die VMware-Instanz auf dem Wirt ablegen. Es könnte zu einem Überlaufen der Platten im ESX kommen. Man kann sie schließen, indem man das Logging komplett abschaltet oder die Dateien in der Größe einschränkt.

Da das VC oft aus mehr als einem Außennetz erreichbar sein soll, entsteht schnell ein Sicherheitsrisiko. Es gelten die Regeln für die Härtung eines Windows Server an besonders exponierter Stelle, wie sie diverse Best Practice Guides und der IT-Grundschutzkatalog des BSI [e] aufführen. Gleiches, in leicht abgeschwächter Form, gilt für den Datenbankserver. Selbst wenn er nicht aus dem Intranet oder dem Verwaltungsnetz erreichbar sein sollte, gilt er wegen der brisanten Daten als primäres Ziel für Angreifer und braucht einen dementsprechenden Schutz. Nach dem Installieren des VC kann man den DB-User, mit dem das VC auf die Datenbank zugreift, in seinen Rechten stark beschneiden.

Für die Sicherheit der gesamten Umgebung sind die Clients relevant, die als Arbeitsplätze der Administratoren fungieren. Wenn dort ein Angreifer einen Keylogger installieren kann, hebelt das alle anderen Sicherheitsmaßnahmen der VI aus, da er mit den Admin-Rechten auf das VC oder den ESX zugreifen kann. Dem sollte man ausreichend Achtung schenken und sich an die Empfehlungen für die Windows-Clients halten. Letztlich bleiben die VMs, die denselben Schutz wie Root-Server genießen sollten.

Sicherheit des Massenspeichers

Das Datenvolumen in einer VI ist erheblich, unter anderem, weil der ESX Server es nicht wie seine kleineren

Brüder erlaubt, die virtuellen Festplatten (*vmdk*-Dateien) dynamisch bis zur maximal eingestellten Grenze zu vergrößern, sondern beim Anlegen des Massenspeichers für die VM eine Datei erzeugt, die genauso groß ist, wie sie dort erscheint. Nur für Tests und kleine Installationen kann man deswegen die lokalen Festplatten des ESX für eine VM nutzen, kann dann aber nicht die erweiterten Funktionen der VI wie High Availability, Distributed Resource Scheduler und VMotion nutzen. Es bedarf eines Speichermediums, das allen ESX einer Farm gleichzeitig zur Verfügung steht. VI unterstützt SAN über Fibre Channel (FC) oder seit der Version 3 über iSCSI.

Per LUN separiert

Der Zugriff ins SAN geht über HBAs (Host Bus Adaptors), die im ESX eingebaut sind. Sofern das SAN es unterstützt, erkennt ESX unterschiedliche Pfade zur gleichen LUN und stellt sie automatisch bereit. Bewährt hat es sich, LUNs mit unterschiedlichen SAN-Architekturen für VMs anzubieten, die voneinander abweichende Sicherheitsanforderungen haben. Nicht jede VM benötigt eine über mehrere Standorte gespiegelte LUN oder eine, die als RAID 5 realisiert ist. So kann man Test-VMs und Entwicklungsumgebungen auf LUNs lagern, die weniger aufwendig sind als diejenigen, die auf Ausfallsicherheit getrimmt sind.

Innerhalb der LUNs richtet das System entweder eine VMFS-Partition ein oder gibt die LUN direkt an die VM per „Raw Device Mapping“ (RDM) weiter. Letzteres erlaubt sogar den Betrieb mancher SAN-Verwaltungssoftware in einer VM, während man gleichzeitig Snapshots für die Daten in der LUN erstellen kann. VMs, deren Cluster-Lösung (etwa Windows Cluster) gemeinsam genutzte LUNs benötigen, sind mit RDM realisierbar.

Schwachpunkt *mount*

Rechte auf den VMs verwaltet ESX auch über Dateisystemrechte. Wer ein VMFS per *mount* einhängen kann, weil er Zugang zu dessen LUN hat, kann die Kontrolle über eine VM übernehmen, obwohl die im VC eingestellten Regeln das verbieten. In einer VI mit mehreren Farmen dürfen auf jedem Host nur die für ihn bereitgestellten LUNs sichtbar sein. Das gilt auch für ESX Server, die zu keiner Farm gehören. Nur eine genaue Planung und Abstimmung der SAN-Zonen und der im SAN angewendeten Masken kann zu einer sauberen Trennung der einzelnen Systeme führen – unter der Voraussetzung, dass das Sicherheitskonzept des SAN das unterstützt.

Auf ihre virtuellen Netze sollten ausschließlich die VMs zugreifen dürfen. Eine Vermischung mit denen der VI ist nicht empfehlenswert, deswegen sollte niemand beim Installieren Default Port Groups einrichten, da sonst die Gefahr besteht, dass jemand in einer VM das Netzwerk des COS oder der gesamten VI-Komponenten sieht.

Für die VMs stellt der jeweilige ESX einen virtuellen Switch (vSwitch) oder eine physische Netzwerkkarte im Server zur Verfügung. Außerdem kann man einen eingehenden VLAN-Trunk auf die Netzwerkkarten der VMs verteilen. ESX agiert als Switch, der einzelne Ports einem VLAN zuordnet. Für die Sicherheitskonzeption ist relevant, dass VMs mit hohen Anforderungen an die Ausfallsicherheit mehr als eine physikalische Netzwerkkarte nutzen. Das kann über eine direkte Zuordnung per Bridging geschehen. Da ein ESX Server sich erst ab vier VMs rentiert, wäre der Bedarf an Karten im Rechner enorm.

Deshalb schließt man üblicherweise die VMs an einen virtuellen Switch an, der wiederum mit bis zu acht physischen Netzwerkkarten an einem oder mehreren physischen Switches angeschlossen ist. Die Netzwerkkarten arbeiten parallel, wobei jede MAC-Adresse eines VM-Ports nur auf einer physischen Netzwerkkarte aktiv sein kann, damit es nicht zu Fehlfunktionen im Netz kommt. Außerdem ist eine Kanalbündelung möglich.

Man kann im ESX für die „Virtual Machine Network Interface Card“ (VMNIC) den VMs den Wechsel der MAC-Adresse verbieten. Wobei „verbieten“ das falsche Wort ist: Wie bei der Port-Security für Switches nimmt ESX den Port in dem Augenblick vom Netz, in dem sich dort beim Senden die MAC-Adresse ändert. Erst wenn wieder die ursprüngliche Adresse in den Ethernet Frames auftaucht, leitet das System sie an die anderen VMs an derselben VMNIC und an die physikalischen Netzwerkkarten weiter. Darüber hinaus kann der Administrator den Promiscuous Mode, in dem alle empfangenen Pakete auf dem Kabel zu sehen sind, den VMs verwehren.

Benannte VMNICs helfen

Wichtig, wenn auch nur für VMotion, ist, dass auf allen ESX Servern einer Farm die gleichen VMNIC vorhanden sein müssen, damit die VMs nach und während eines Umzugs ihren Kontakt zu ihrem Netz nicht verlieren. Es empfiehlt sich außerdem, die VMNICs sprechend zu benennen. ESX hilft in der GUI, indem es dort die auf der Karte per Sniffer entdeckten IP-Nummern der angeschlossenen Netze anzeigt, sodass man die VMs den richtigen VMNICs leicht zuordnen kann.

Sicherheit heißt in diesem Kontext nicht nur, die VI vor den VMs zu schützen und Letztere vor Malware, Angreifern und allem, was die Trennung der VMs voneinander und die dort gelagerten Daten verändern könnte, sondern auch für Verfügbarkeit zu sorgen.

Um zu verhindern, dass eine VM alle verfügbaren Ressourcen aufbraucht, kann der Systembetreuer für jede VM eine Ober- und Untergrenze für den Gebrauch der Ressourcen setzen. Obergrenzen für produktive VMs sind nur bedingt sinnvoll, da sie bei kurzfristigen Leistungsspitzen nicht mehr reagieren können. Solche, bei denen es im selben Zeitraum zu hohen Lasten kommen kann, sollten prophylaktisch auf unterschiedlichen ESX laufen. Dabei kann VMwares „Distributed Resource Scheduler“ helfen, da bei einem Lastengpass einer VM die VI darauf reagieren und die virtuelle Maschine auf einen nicht ausgelasteten Servern, verlagern kann.

Fazit

Bei Beachtung aller Sicherheitsmaßnahmen, einem überwachten Betrieb und schnellen Prozessen zum Beheben von Schwierigkeiten ist VMwares Virtual Infrastructure den Anforderungen der Sicherheit an den Betrieb mit produktiven Anwendungen und sensiblen Daten gewachsen. Jedoch wächst der Grad der Komplexität durch die zusätzliche Software und die damit verbundenen administrativen Aufgaben.

VMware schlägt vor, aus Gründen der Lastverteilung, auf einem ESX produktive VMs mit Test- und Entwicklungsumgebungen gleichzeitig zu betreiben, da die beiden Letztgenannten nur selten Ressourcen verbrauchen und viele Speicherseiten mit iden-

tischem Inhalt erzeugen, der nur einmal pro ESX physikalisch existieren muss. Das führt zu einer besseren Auslastung der gesamten Hardware. Zwar sprechen unter Sicherheitsaspekten derzeit kaum Gründe gegen den Einsatz des ESX, trotzdem will ein solcher Schritt gut überlegt sein und nur für VMs gewählt werden, deren Anforderungen an die Sicherheit nicht zu hoch sind.

Ähnliches gilt für die Vermischung von VMs aus Zonen mit unterschiedlichen Sicherheitsanforderungen in einer durch Firewalls aufgeteilten Umgebung, etwa die unterschiedlichen Segmente einer DMZ. Nach dem derzeitigen Kenntnisstand beeinträchtigt die Virtualisierung die Sicherheit der VMs in einer solchen Architektur gering, erhöht sie sogar unter Umständen, da man Konzepte wie Ausfallsicherheit in der VI mit weniger Aufwand und gleich für mehrere Systeme realisieren kann. Trotzdem bestehen Gefahren, wie sie durch unabsichtliche Fehlkonfigurationen oder Fehler in der Virtualisierungstechnik entstehen können. VMs, deren Sicherheitsklassen weit auseinanderliegen, sollten auf keinen Fall zur selben VI gehören. (rh)

CHRISTOPH PUPPE

ist Sicherheitsberater bei der HiSolutions AG, Berlin.

Onlinequellen

[a] Evaluation Assurance Level	www.commoncriteria.de/index.php?option=com_content&task=view&id=8&Itemid=60
[b] Protection Profiles	www.commoncriteria.de/index.php?option=com_content&task=view&id=9&Itemid=2
[c] Common Criteria	www.commoncriteriaportal.org
[d] Verwundbarkeit von VI3	archives.neohapsis.com/archives/fulldisclosure/2007-09/0356.html
[e] Windows Server härten	www.bsi.de/gshb/deutsch/baust/b03108.htm

Literatur

[1] Sven Ahnert; Virtualisierung; Transparente Verbindlichkeiten; Stärken und Schwächen von VMwares Infrastructure 3; *iX* 9/2007, S. 70

[2] Stefan Gora; Rootkits; Bittere Pille; Schadsoftware beutet Hardware-Virtualisierung aus; *iX* 4/2007, S. 120

[3] Alexander Geschonneck; Computerforensik; Wiederbelebung; Festplatten-Images mit Live View unter VMware analysieren; *iX* 4/2007, S. 139

[4] Michael Ziegler; Virtualisierung; Desktop zentral; VMwares Konzept der Virtual Desktop Infrastructure; *iX* 8/2006, S. 110

[5] David Ochel; Zertifizierung; Garantiert sicher; Evaluierung von IT-Sicherheit; *iX* 5/2005, S. 132



Dateien vergleichen und synchronisieren

Apfel oder Birne

Roland Schmitz

In vielen Fällen ist es unmöglich oder zu mühsam, Dateien manuell zu vergleichen: Sie liegen in einem nicht lesbaren Format vor, sind zu groß oder die Unterschiede zu unscheinbar. Oft helfen Standardwerkzeuge wie Gimp oder Emacs, doch manchmal müssen auch die Spezialisten ran.

Vielfach kommt es vor, dass man wissen möchte oder muss, ob sich eine Datei gegenüber einem gesicherten Stand verändert hat. Ein Grund dafür kann sein, dass mehrere Personen an einem Text oder Skript arbeiten oder man prüfen will, ob die lokale Kopie identisch ist mit der, die auf dem Server liegt. Softwaretests können ein weiterer Grund dafür sein, etwa wenn man prüfen muss, ob die neue Version eines Programms dieselben Ergebnisse liefert wie die alte. Die hier genannten Werkzeuge sind nur als Auswahl zu verstehen, die nicht zuletzt von persönlichen Vorlieben geprägt ist. Bei den genannten Vergleichstools etwa gibt es vielfach auch grafische Varianten. Im Fokus dieses Artikels stehen jedoch weniger die Tools und deren Bedienung, als vielmehr die geeignete „Wahl der Waffen“.

Am häufigsten sind es wohl Textdateien, die man vergleichen will. Da sie für Menschen lesbar sind, erscheint die Aufgabe auf den ersten Blick banal. Spätestens aber, wenn die Dateien groß, unübersichtlich oder die Änderungen umfangreich sind, wäre ein manueller Vergleich mehr als nur mühsam – und fehleranfällig. Deshalb haben alle größeren Editoren wie *vi*, *emacs* und ihre Clones entsprechende Compare-Funktionen integriert. *xemacs* beispielsweise besitzt ein integriertes *diff*, das wie das Original zeilenweise arbeitet. Es markiert die differierenden Passagen zweier Textdateien, die *xemacs* in zwei über- oder nebeneinander angeordneten Fenstern anzeigt. In dem separaten Buffer **ediff-diff** ist zusätzlich die gewohnte *diff*-Ausgabe zu finden.

Haben sich in einem längeren Text nur einzelne Buchstaben oder Wörter geändert, etwa bei der Rechtschreibkorrektur, oder sind bei den Änderungen die Zeilenumbrüche verrutscht, ist ein zeilenweiser Vergleich völlig ungeeignet. Wenig um Zeilenumbrüche und Formatierungen kümmert sich deshalb *wdiff <datei_alt> <datei_neu>*. Stattdessen vergleicht es zwei Textdateien wortweise und gibt den Text komplett aus. Dabei markiert es an jeder geänderten Passage die alte Version mit *[–<wort1>–]* und setzt direkt dahinter die neue Formulierung, gekennzeichnet mit *{+<wort2>+}*. Alternativ lassen sich die Marken *[–* und *{+* durch eigene ersetzen. Man definiert sie beim Aufruf von *wdiff* mit *--start-delete <marke>* und *--end-delete <marke>* beziehungsweise *--start-insert <marke>* und *--end-insert <marke>*.

Versionskonflike berücksichtigt

Die ungewöhnlichen Marken sind insofern nützlich, als sie sich gut – nachdem man die Ausgabe in eine Datei umgeleitet hat – mit der Suchfunktion jedes beliebigen Editors oder Viewers von *less* aufwärts wiederfinden lassen. Da der komplette Text erhalten bleibt, eignet sich die Ausgabe gegebenenfalls auch für die Weiterverarbeitung. Und wer alle markierten Stellen gleichzeitig hervorgehoben haben will, kann sie im *emacs* oder *vi* als regulären Ausdruck ins Syntax-Highlighting einbauen.

Haben zwei Leute parallel an einem Text oder Skript gearbeitet, lohnt es auf jeden Fall, die Ursprungsversion aufzubewahren. Dann nämlich kann man mit dem Tool *merge* aus dem RCS-Paket die beiden geänderten Versionen zusammenfügen: *merge <version1> <original> <version2>* vergleicht *<version1>* und *<version2>* mit dem Original und schreibt die Änderungen von *<version2>* in *<version1>*, die man deshalb vorher sichern sollte. Haben beide Autoren dieselbe Stelle unterschiedlich bearbeitet, zeigt *merge* den Konflikt an:

```
<<<<<<< version1.txt
Apfel oder Birne
=======
Apfel oder Birne?
>>>>>>> version2.txt
```

den man dann händisch editieren muss.

Zu den Spezialfällen zählen unstrukturierte Dateien, die man zuvor mit *sort* oder *msort* ordnen kann. Zu ihnen zählen etwa alle unsortierten Listen wie die von IP-Adressen. Unliebsame Doppler lassen sich mit *uniq* entsorgen.

Ebenfalls zu den – scheinbar aussterbenden – Spezialfällen zählen Dateien mit fester Satzlänge oder Fixed Record Length Files. Zu finden sind sie noch auf Großrechnern oder in Spezialanwendungen wie Geoinformationssystemen. Sie lassen sich am besten mit darauf spezialisierten Editoren wie dem Flat File Tool oder dem Flat File Editor bearbeiten, auch wenn beide Projekte derzeit nicht übermäßig aktiv sind.

Häufig kommen dagegen ASCII-Tabellen vor, meist in Form von CSV-Dateien (Comma Separated Values), die allerdings nicht zwangsweise das Komma als Trennzeichen verwenden müssen. Vor und nach Tests von Datenbankanwendungen etwa sichert man in der

Regel den Datenbestand zum anschließenden Vergleich. Da sich Binärdateien dazu nicht wirklich eignen, werden diese DB-Dumps oft als CSV-Dateien erstellt.

Zwar lassen sich CSV-Dateien mit jedem beliebigen Editor öffnen, doch sind sie dort meist unübersichtlich dargestellt, da die Felder meist unterschiedlich lang sind. Übersichtlicher wird die Ansicht mit Tabellenkalkulationsprogrammen wie OpenOffice.org Calc, mit CSV-Editoren wie CSVed für Windows oder dem Record-Editor, da sie mit den Eigenheiten der CSV-Dateien vertraut sind. Zum Vergleichen eignet sich besonders das Perl-Skript *csvdiff*.

```
perl csvdiff.pl –a neu.csv –e alt.csv –s ";" ↙
                              –k "2" –t –i 2>&1
```

gibt alle abweichenden Einträge mit Schlüssel sowie Nummer und Inhalt von Zeile und Feld aus. Während *–s* das zu verwendende Trennzeichen bestimmt, definiert *–k* die Schlüssel-Spalte; *–t* (trim) schneidet die Leerzeichen am Anfang und am Ende weg und *–i* veranlasst das Skript dazu, die Groß- und Kleinschreibung zu ignorieren.

Nichtlesbares vergleichen

Ebenfalls häufig vertreten sind XML-Dateien, die wie CSV-Dateien eine eigene Struktur aufweisen. *XmlDiff* und *Libxmldiff* heißen zwei der Programme zum Vergleichen von XML-Dateien. Sie unterscheiden sich vor allem in der Art und Weise, wie sie das Vergleichsergebnis präsentieren. *Libxmldiff* gibt das Ergebnis in derselben Struktur wie die beiden Eingabedateien aus, fügt jedoch ein zusätzliches Attribut *diff:<status>* ein, wobei der Status *added*, *removed*, *modified* oder *below* sein kann. *XmlDiff* arbeitet wie *diff* und präsentiert als Ergebnis eine Reihe von Aktionen, die, wenn sie angewendet werden, dazu führen, dass beide Dateien identisch sind.

Schwieriger gestaltet sich ein Vergleich von Multimedia- oder Binärdateien. Hier kommt man mit den klassischen Editoren wie *vi*, *emacs* oder deren Clones und Alternativen nicht sehr weit – trotz ihrer integrierten Compare-Funktionen. Geeigneter sind dort schon Hex-Viewer und -Editoren wie *od*, mit denen man die Dateien ansehen und somit auch vergleichen kann.

Aber wenn es lediglich darum geht, ob die Dateien gleich sind, kann man ebenso den *md5*-Fingerprint dazu heranziehen. Auch die „üblichen Verdächtigen“ wie *cmp* und *diff* sind hier nicht besonders hilfreich: Während *diff* sich bei Binärdateien gerade einmal zu der Aussage bewegen lässt, dass sich die Dateien unterscheiden, gibt *cmp* zumindest die erste Stelle bekannt, an der ein Unterschied aufgetreten ist:

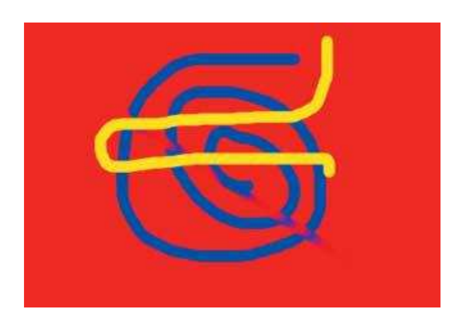
```
$ cmp datei1 datei2
datei datei2 differ: char 28, line 2
```

Allerdings reicht das nicht aus, um den Unterschied bewerten zu können. Besteht der Verdacht, dass *cmp* auf unterschiedliche Zeitstempel sonst gleicher Binaries hereinfällt, kann man das Kommando mit *--ignore–initial=16* dazu bewegen, den Header zu ignorieren.

Unterschiedlichen Versionen einer Binärdatei kann man mit dem Befehl *xdelta* beikommen. Er erzeugt ein sogenanntes Delta mit den (rekursiven) Unterschieden der beiden Versionen, das sich bei Gelegenheit als Patch benutzen lässt. Für die einzelnen Schritte benutzt es Subkommandos: *xdelta delta <old_version> <new_version> output* erzeugt das Delta, *xdelta info output* gibt Informationen darüber aus und *xdelta patch output <oldversion> <newfile>* rekonstruiert *<new_version>* und schreibt sie in *<newfile>*. Lässt man die Angabe von *<newfile>* weg, schreibt *xdelta* die Rekonstruktion in *<new_version>.xdp1*

Auch für Bilder kann man ein Differenzbild erstellen. Hierzu steht der ImageMagick-Werkzeugkasten bereit, oder – wie sollte es anders sein – Gimp. Dazu muss man in Gimp die beiden Bilder als Ebenen übereinanderlegen, indem man Bild 1 öffnet und über das Datei-Menü von Bild 1 das zweite Bild als Ebene öffnet. Im Dialoge-Menü des Bildes wählt man nun den Dialog „Ebenen“. Dort ändert man den Modus für das soeben geöffnete Bild 2 von „Normal“ auf „Unterschied“. Dasselbe Ergebnis – also ein identisches Differenzbild – liefert das ImageMagick-Tool *convert*, ein ähnliches sein Bruder *compare*:

```
convert image1.png image2.png –compose↙
              difference –composite output.png
compare image1.png image2.png output.png
```



Die Spirale im Originalbild wird rechts und links um jeweils 5 Pixel verkürzt (Abb. 1a).



Das von Gimp erzeugte Differenzbild stellt die Unterschiede farbig dar (Abb. 1b).

Als Beispiel wird die Spirale in Abbildung 1a links und rechts um jeweils fünf Pixel beschnitten, sodass der Unterschied mit dem bloßen Auge nicht sichtbar ist. Im Ergebnis ist die Spirale in der Horizontalen nur zehn Pixel schmaler.

Die von Gimp und *convert* erzeugten Differenzbilder zeigen die Unterschiede farbig und die identischen Stellen schwarz an, in dem von *compare* erzeugten bleiben die identischen Passagen weiß. Welche Schlüsse man dem Differenzbild allerdings ziehen kann, ist von Fall zu Fall unterschiedlich.

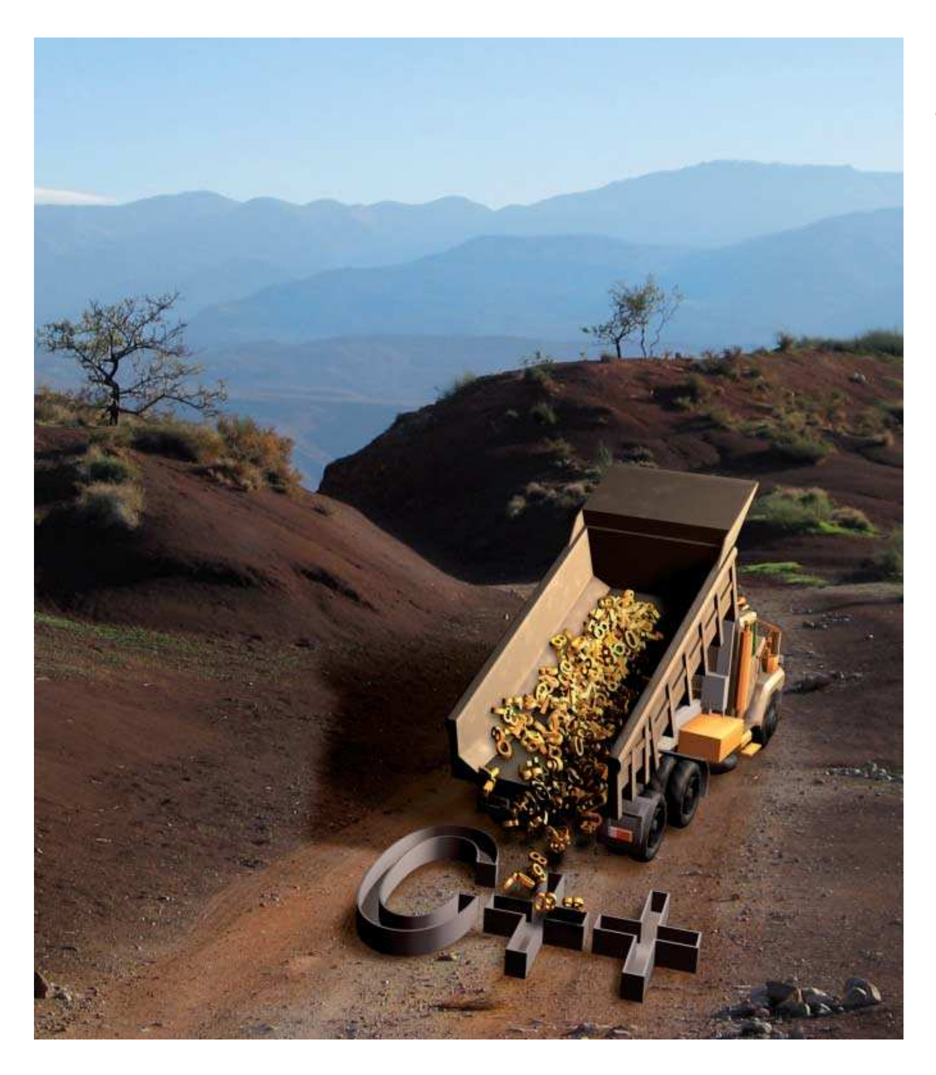
Für WAV-Dateien ist auf Sourceforge das Tool FourierRocks zu finden, das per Spektralanalyse ermittelt, inwieweit sich die beiden Dateien gleichen. (sun)

ROLAND SCHMITZ

beschäftigt sich bei der Corporate Quality Consulting GmbH mit Softwarequalitätssicherung und Prozessberatung.

Onlinequellen

CSVed	home.hccnet.nl/s.j.francke/t2t/text2table.htm
csvdiff	csvdiff.sourceforge.net
Flat File Editor	sourceforge.net/projects/ffe
Flat File Tool	fftool.sourceforge.net
Gimp	www.gimp.org
Gtkdiff	home.catv.ne.jp/pp/ginoue/software/gtkdiff/index-e.html
ImageMagick	www.imagemagick.org
Kdiff3	kdiff3.sourceforge.net
Kompare (Kdiff)	www.caffeinated.me.uk/kompare
Libxmldiff	people.via.ecp.fr/~remi/soft/xml/libxmldiff/libxmldiff_en.php3
merge	www.gnu.org/software/rcs
msort	freshmeat.net/projects/msort
Record-Editor	record-editor.sourceforge.net
wdiff	www.gnu.org/software/wdiff
xdelta	xdelta.org
XmlDiff	www.logilab.org/projects/xmldiff



Boost-Tutorial III: Serialisierung und Netzprogrammierung

Warten auf den Zufall

Rüdiger Berlich

Zwar ist die Vernetzung von Computern kein neues Phänomen, aber die Programmierung verteilter Anwendungen stellt noch immer hohe Anforderungen an Programmierer. Der dritte Teil dieses Tutorials beschreibt, wie in C++-Anwendungen Boost-Klassen den Austausch von Nachrichten zwischen Client und Server erleichtern, bei der Generierung von Zufallszahlen helfen und die Serialisierung ermöglichen.

Man sollte meinen, dass in Betriebssystemen und Programmiersprachen die Einbindung verteilter Ressourcen heute ähnlich selbstverständlich ist wie die Darstellung von Grafik auf dem Bildschirm. Auch hier werden komplexe und von der jeweiligen Umgebung abhängige Arbeitsschritte durchlaufen, von denen der Online-Spieler höchstens das Zucken seines virtuellen Monsters nach dem Schuss eines anderen Monsters bemerkt. Wenn beide Monster sich auf verschiedenen Rechnern befinden, muss man sich fragen, wie sie miteinander kommunizieren. Vielleicht wird, möglicherweise auf einem dritten Rechner, eine Server-Instanz den Weg von Kugel und Monster 2 verfolgen, um festzustellen, ob sich beide zu irgendeinem Zeitpunkt am selben Ort befanden. Dies setzt den Austausch von Nachrichten voraus. Und genau diese Kommunikation erfordert leider oft noch erhebliche Feinarbeit.

Dieser dritte Teil des Boost-Tutorials beschäftigt sich mit der Frage, wie man unter C++ mit Boost die Kommunikation zwischen verteilten Programmen gestaltet. Um dieses Hauptthema ranken sich Informationen zur Serialisierung von Objekten und zur Generierung von Zufallszahlen.

Nicht alles dem Zufall überlassen

Von Computerprogrammen erwartet man voraussagbares Verhalten, wenn sie mit den gleichen Randbedingungen starten. So etwas wie „echte Zufallszahlen“ bekommt man von einem Computer also nur dann, wenn der Algorithmus Zugriff auf eine Quelle nicht vorhersagbarer Werte hat. In der Realität wird man sich meist mit weniger zufriedengeben müssen.

Generatoren liefern ihre Zahlen oft als gleich verteilte Integer-Zahlen im gesamten Wertebereich des Basistyps oder als ebenfalls gleich verteilte Floatingpoint-Zahlen auf einem Intervall (meist [0,1]). Viele Anwendungen benötigen aber spezielle Verteilungen. So verlangen beispielsweise Evolutionsstrategien zufällige Gleitkommazahlen, die eine Gaußverteilung aufweisen.

Hier hilft *Boost.Random* (Header: *<boost/random.hpp>*), eine Sammlung unterschiedlicher Generatoren, die sich mit Klassen zur Berechnung vieler Verteilungen kombinieren lassen.

Das Prinzip ist einfach, die Beschreibung auf der Boost-Hompage (siehe „Onlinequellen“ [a]) allerdings sehr technisch.

Listing 1 liefert eine Einführung in diese Thematik. Zunächst erzeugt es jeweils einen Generator für Zufallszahlen nach dem Mersenne-Twister- und dem Linear-Congruential-Algorithmus. Den Startwert bezieht das Programm jeweils aus der aktuellen Zeit.

Es folgen Objekte für eine Gleich- und eine Normalverteilung. Erstere soll Werte im Bereich [0,7] ausgeben, die Normalverteilung solche mit dem Mittelwert 0 und einer kumulierten Breite von 1.

Der nächste Schritt verbindet Generator und Verteilung, indem er sie als Argumente an ein Objekt des Typs *variate_generator* übergibt. So wird ein Funktionsobjekt definiert, das beim Aufruf Zufallszahlen der gewählten Verteilung zurückgibt. Die Zeilen in Abbildung 1 demonstrieren dies. Aus Gründen der Darstellung sind die Nachkommastellen auf 2 beschränkt.

Man sollte einige Zeit einplanen, um sich in die Thematik einzuarbeiten. Zum einen erfordert die Beschreibung auf der Webseite einiges an Vorkenntnissen. Zum anderen kommt der Wahl des Algorithmus eine entscheidende Bedeutung zu. Hier muss eine Abwägung zwischen der Geschwindigkeit des Generators und der Qualität der erzeugten Zufallszahlen erfolgen.

Es sei noch darauf hingewiesen, dass die *uniform_real*-Verteilung laut ihrer Beschreibung einen Fehler aufweist. In den Tests war sie jedoch problemlos zu verwenden. Die Entwicklung von Boost ist so dynamisch, dass dieser Fehler in absehbarer Zeit behoben sein sollte.

Man stelle sich nun eine Rechenumgebung mit häufigen Stromausfällen vor. In solchen Fällen wäre es vorteilhaft, den Zustand einzelner Objekte auf der Festplatte zwischenzuspeichern, um sie zu einem späteren Zeitpunkt aus diesen Daten wieder rekonstruieren zu können. Diese Umwandlung zwischen Objekten und Text- oder Binärdarstellungen leistet *Boost.Serialization*.

iX-TRACT

- Funktionen der Boost-Bibliothek helfen C++-Programmierern unter anderem bei der Kommunikation zwischen verteilten Programmen.
- Eine Beispielanwendung demonstriert, wie unterschiedliche Generatoren Zufallszahlen produzieren, die sich durch Objekte unterschiedlichen Typs serialisiert darstellen lassen.
- Eine Client-Server-Anwendung überlässt das Sortieren der Zahlen dem Client, der die Daten zur Weiterverarbeitung an den Server zurücksendet.

Serienproduktion über den Stream-Operator

In Standardsituationen ist die Anwendung denkbar einfach. Listing 2 demonstriert zunächst die Serialisierung eines *vector* mit drei Zahlen.

Boost.Serialization umfasst verschiedene Archivklassen, deren Konstruktoren jeweils ein *ostream*- respektive *istream*-Argument oder davon abgeleitete Klassen erwarten (je nachdem, ob es sich um die Generierung oder das Lesen eines Archivs handelt). Dies würde es erlauben, als Zielmedium etwa einen *ofstream* zu verwenden und die Ausgabe direkt in eine Datei auf der Festplatte umzuleiten. Stattdessen soll hier aber ein *stringstream* einen direkten Zugriff auf die serialisierte Darstellung des *vector* ermöglichen.

Da das Archiv im XML-Format vorliegen soll, wird ein *xml_oarchive*-Objekt erzeugt, dem ein *ostringstream* übergeben wird. Neben der XML-Darstellung von Objekten existiert eine eigene Darstellung ohne die XML-typischen Tags. Sie besitzt damit deutlich weniger Overhead, ist allerdings für manuelle Änderungen wenig geeignet. Die Speicherung der Objektinformationen im Binärformat ist eine weitere Alternative.

Die eigentliche Serialisierung erfolgt über den Stream-Operator: *oa << make_nvp(„simple“,simple);*. *make_nvp* steht für „make name/value pair“ und ordnet einem Objekt die XML-typischen Tags zu.

Boost.Serialization kennt die Algorithmen der Standard Template Library. Die Bibliothek besitzt zudem eine umfassende Sammlung weiterer Datenstrukturen insbesondere aus dem Boost-Umfeld. Entwickler müssen sich daher nicht die Mühe machen, einen *shared_ptr* zu beschreiben. Das darin referenzierte Objekt muss natürlich

Listing 1: Generierung von Zufallszahlen

```
int main(int argc, char** argv){
  // Mersenne Twister
  mt19937 mersenne(static_cast<unsigned int> (time(0)));
  // Linear Congruential
  minstd_rand0 linearCongruential(static_cast<unsigned int> (time(0)));
  // Uniform distribution
  uniform_real<double> evenDist(0.,7.);
  // Normal/Gaussian distribution
  normal_distribution<double> normalDist(0.,1.);
  // Combination of generators with distributions
  variate_generator<mt19937&, uniform_real<double> >
                        even(mersenne, evenDist);
  variate_generator<minstd_rand0&, normal_distribution<double> >
                        gauss(linearCongruential, normalDist);
  // Output
  cout.precision(2);
  cout << "Even distribution [0,7[ :" << endl;
  for(unsigned int i=0; i<10; i++) cout << fixed << even() << " ";
  cout << endl;
  cout << "Normal distribution with mean 0 and sigma 1 :" << endl;
  for(unsigned int i=0; i<10; i++) cout << gauss() << " ";
  cout << endl;
  return 0;
}
```

```
Even distribution [0,7] :
1.50 1.82 0.94 3.03 5.35 2.61 1.96 4.16 1.71 3.81
Normal distribution with mean 0 and sigma 1 :
0.12 1.98 -0.41 0.48 -1.83 0.28 -0.54 -1.21 0.68 -0.19
```

Zufallszahlen, mit unterschiedlichen Algorithmen und Verteilungen generiert (Abb. 1)

Listing 2: Serialisierung eines *vector*

```
int main(int argc, char **argv){
  vector<int> simple;
  // Fill vector<int> with values
  for(int i=0; i<3; i++) simple.push_back(i);

  // Serialize
  ostringstream oss;
  {
    xml_oarchive oa(oss);
    oa << make_nvp("simple",simple);
  }
  // Let the audience know
  cout << "XML description of \"simple:\"" << endl << endl
       << oss.str() << endl;
  // Fill XML code back into another vector<int>
  vector<int> simple2;
  istringstream iss(oss.str());
  {
    xml_iarchive ia(iss);
    ia >> make_nvp("simple",simple2);
  }
  // Show the content of the new object
  cout << "Content of \"simple2:\"" << endl;
  for(int i=0; i<simple2.size(); i++) cout << simple2[i] << " ";
  cout << endl;
}
```

```
<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
<!DOCTYPE boost_serialization>
<boost_serialization signature="serialization::archive"
version="4">
<simple>
        <count>3</count>
        <item_version>0</item_version>
        <item>0</item>
        <item>1</item>
        <item>2</item>
</simple>
</boost_serialization>
```

Die XML-Beschreibung des Vektors *<simple>* (Abb. 2)

Listing 3: *secretNumber*-Klasse

```
class secretNumber
{
  ///////////////////////////////////////////////////////////////
  friend class boost::serialization::access;

  template<class Archive>
  void serialize(Archive & ar, const unsigned int version){
    using boost::serialization::make_nvp;
    ar & make_nvp("secret_", secret_);
  }
  ///////////////////////////////////////////////////////////////

public:
  secretNumber(void) : secret_(0) { /* nothing */ }
  secretNumber(double secret) : secret_(secret) { /* nothing */ }
  double value(void) const { return secret_; }
private:
  double secret_;
};
```

Listing 4: *base*-Klasse

```
template <class T>
class base
  :public vector<T>
{
  ///////////////////////////////////////////////////////////////
  friend class boost::serialization::access;
  template<class Archive>
  void serialize(Archive & ar, const unsigned int version){
    using boost::serialization::make_nvp;
    ar & make_nvp("stdvector", boost::serialization::base_object<vector<T> >(*this));
  }
  ///////////////////////////////////////////////////////////////
public:
  virtual void sort(void) = 0;
};
namespace boost {
  namespace serialization {
    template<class T>
    struct is_abstract<base<T> > {
      typedef mpl::bool_<true> type;
      BOOST_STATIC_CONSTANT(bool, value = true);
    };
}}
```

serialisierbar sein. Auch im vorliegenden Beispiel ist es nicht notwendig, den Serialisierer über die inneren Strukturen eines *vector* aufzuklären.

Wichtig sind die geschweiften Klammern um die Serialisierung. Sie sorgen für die Zerstörung der *xml_oarchive*-Objekts nach der Serialisierung. Hierbei wird der Destruktor von *xml_oarchive* aufgerufen, der die passenden schließenden Tags in das XML-Archiv schreibt.

Der nächste Schritt gibt den serialisierten Vektor auf der Konsole aus. Nach dem Header – er markiert die Ausgabe als *Boost.Serialization*-Archiv einer gegebenen Version – folgt die XML-Repräsentation des *vector*. Das abschließende *</boost_serialization>* würde fehlen, wenn nicht geschweifte Klammern die Serialisierung umschließen würden.

Anschließend wird ein neuer (leerer) *vector<int>* erzeugt, in den das XML-Archiv über ein *istringstream*-Objekt hineingeladen wird. Dabei muss der Anwender die Details dieses Prozesses nicht kennen. Er verwendet einfach den Stream-Operator „>“.

Zu guter Letzt erfolgt die Ausgabe des Inhalt des neuen Vektors auf der Konsole. Sie lautet wie erwartet *0 1 2*.

Etwas Handarbeit muss auch sein

Das nächste Beispiel (Listing 3) erstellt eine Klasse *secretNumber*. Sie enthält als private Komponente eine Double-Zahl, die über einen Konstruktor gesetzt und über die Funktion *value()* abgefragt werden kann.

Auffällig sind die Zeilen im Kopfteil. *Boost.Serialization* erhält hier Zugang zu den geschützten Teilen der Klasse. Ferner wird hier eine Memberfunktion *serialize* erstellt. Dieser Funktion muss das Programm bekannt geben, dass es ein Datenelement *secret_* in der Klasse gibt. Generell beschreibt man hier alle Daten und Objekte, die zur Erstellung eines Objekts des serialisierten Typs notwendig sind. Der Entwickler kann aber auch eigene Aktionen anstoßen. So wäre es möglich, einen Eintrag in ein Logfile zu schreiben, sobald ein Objekt dieses Typs (de-)serialisiert wird.

Als nächste Komponente wird die Klasse *base* erzeugt (Listing 4). Sie leitet sich von einem *vector* ab, dessen Serialisierung bereits erläutert wurde. Die Ableitung von einem Container der STL würde keinen Preis für gute Programmierung einbringen, ermöglicht aber eine vereinfachte Darstellung für diesen Artikel.

Boost.Serialization muss darüber Kenntnis erhalten, dass es eine Elternklasse gibt, die es zu serialisieren gilt. Bei deren Umwandlung greift die Bibliothek entweder auf die Serialisierungsspezifikationen der Elternklasse oder auf externe Spezifikationen zurück. Im Falle von *vector* sind diese in der einzubindenden Header-Datei *<boost/serialization/vector.hpp>* enthalten. Die Serialisierung erfordert die Einbindung ungewöhnlich vieler Header-Dateien. Informationen über die benötigten Dateien sind dem Gesamtlisting dieses Beispiels zu entnehmen, das über den *iX*-Listingservice erhältlich ist.

Der Ausdruck *base_object<vector<T> >(*this)* macht in *base<T>::serialize()* die Elternklasse bekannt. Gäbe es mehrere Elternklassen, könnte man auch mehrere solcher Ausdrücke angeben.

Da *base* als Template implementiert ist, weiß man nicht, welche Daten die Klasse speichert. Die Memberfunktion *sort()* muss damit rein virtuell sein, und Objekte dieser Klasse sind nicht instantiierbar. Bezüglich der Serialisierung ist das Beispiel deshalb alles andere als trivial. Es wäre übrigens durchaus möglich, *shared_ptr* auf Objekte dieses Typs in einem Vektor zu speichern und diese (Smart-)Pointer auf abgeleitete Klassen zeigen zu lassen. *Boost.Serialization* ist in der Lage, mit dieser Situation umzugehen und solche Vektoren zu (de-)serialisieren.

Templates und abstrakte Klassen

Den Bibliotheksfunktionen muss mitgeteilt werden, dass es sich bei *base* um eine abstrakte Klasse handelt. Für „normale“ abstrakte Klassen würde man diesen Hinweis über das Makro *BOOST_IS_ABSTRACT(myClass)* geben. Leider funktioniert das nicht für Templates. Der Programmierer muss den im Makro enthaltenen Code deshalb gewissermassen von Hand angeben. Dies geschieht am Ende von Listing 4.

Details zu *BOOST_IS_ABSTRACT* und zu anderen „Type Traits“ sind auf der Boost-Website zu finden [b]. Ein weiteres wichtiges Makro ist *BOOST_CLASS_EXPORT_GUID(my_class, "my_class_external_identifier")*. Es wird benötigt, wenn man abgeleitete Klassen über einen Zeiger auf ihre Basisklassen (de-)serialisieren will. Mehr zu diesem Thema findet sich ebenfalls im Web [c].

Um in diesem Tutorial möglichst viele Fälle abzudecken, ist die *base*-Klasse etwas konstruiert. Man hätte

beispielsweise auch auf die *sort()* Funktion der STL zurückgreifen können (eine entsprechende Metrik vorausgesetzt).

Serialisieren hilft beim Kommunizieren

Im nächsten Schritt geht es darum, eine Klasse von *base<T>* abzuleiten (Listing 5). Sie ist das eigentliche Serialisierungsziel und leistet auch in der Netzkommunikation gute Dienste. Ziel ist es, in der Subklasse Objekte des Typs *shared_ptr<secretNumber>* zu speichern. Entsprechend wird *secretContainer* von *base<shared_ptr<secretNumber> >* abgeleitet.

Die Klasse besitzt durchaus lokale Objekte – einen Zufallszahlengenerator und eine Verteilung – jedoch sollen diese nicht serialisiert werden. Stattdessen initialisiert das Beispiel den Generator für jedes neue Objekt des Typs *secretContainer* im Konstruktor mit der aktuellen Zeit. In *secretContainer::serialize()* muss deshalb nur die Elternklasse angegeben werden.

Der Konstruktor füllt das Objekt mit einer Anzahl *size* von Zufallszahlen. Hier kommt der Mersenne-Twister-Generator zusammen mit einer Normalverteilung zum Einsatz.

Es folgen zwei Funktionen *toString()* und *fromString*, die lediglich den Code zur (De-)Serialisierung kapseln. Sie dienen eher der Lesbarkeit der *main()*-Funktion. Über ein *#define* lässt sich steuern, ob bei der Serialisierung XML-Code oder das bibliothekseigene Ausgabeformat genutzt werden soll. Im Fall von XML benötigt der Compiler nur den Schalter *-DXMLARCHIVE*.

Die Funktion *secretContainer::sort()* spezifiziert nun den Code, der in *base<T>* fehlt, indem sie einfach auf die STL-eigene *sort()*-Funktion zurückgreift. Wie schon in den vergangenen Artikeln wird hier auf *boost::bind* zurückgegriffen, um eine Metrik für die Sortierung anzugeben.

Listing 6 zeigt schließlich die *main()*-Funktion. Für mehr Komfort definiert die Anwendung noch einen eigenen Stream-Operator für *secretContainer*, der hier nicht gezeigt wird. Die *main()*-Funktion ist einfach. Das Listing erzeugt ein *secretContainer*-Objekt, das es mit zehn *shared_ptr<secretNumber>* füllt und sortiert.

Die Hilfsfunktion *toString()* erzeugt eine Textrepräsentation des Objekts und gibt sie auf der Konsole aus. Wie das einfachere Vektorbeispiel lädt dieses Programm den String in ein anderes *secretContainer*-Objekt, dessen Ausgabe erneut auf der Konsole erfolgt. Verwendet man das *text_oarchive* von *Boost.Serialization*, sieht die Ausgabe aus wie in Abbildung 3.

Wegen der Rundung des *operator<<* unterscheiden sich die Ausgaben des zweiten Objekts *sc2* leicht von der serialisierten Version von *sc*. Intern sind sie jedoch identisch.

Spektakulär ist insbesondere, wie unspektakulär die Serialisierung abläuft – das Beispiel ist ja durchaus auf reale Fälle übertragbar. Im Vergleich zur Ausgabe von Listing 2 sollte aber auch ersichtlich sein, dass das gewählte Textformat deutlich weniger Freiraum für manuelle Änderungen lässt.

Noch ein Wort zur Effizienz der Archiverzeugung und zur benötigten Rechenzeit. Ein *secretContainer* mit einer Million Einträgen erzeugt ein Textarchiv von 28 MByte. Im XML-Modus sind es immerhin schon 122 MByte. Verzichtet man auf das Sortieren des Vektors sowie auf die Ausgabe, dauert der gesamte Programmlauf, einschließlich (De-)Serialisierung auf einem Athlon64 6000+ für das reine Textarchiv sieben Sekunden. Im Falle des XML-Archivs sind es über 16 Sekunden. Das Programm wurde optimiert.

Es ist damit klar, dass sich *text_oarchive* deutlich besser zum Datenaustausch eignet als *xml_oarchive*. Es gibt Binärarchive, die noch effizienter, jedoch nicht unbedingt portabel sind, insbesondere, wenn man einen Datenaustausch über Architekturgrenzen hinweg plant.

Einige der Boost-Datenstrukturen sind nicht ohne Weiteres serialisierbar. Konzeptbedingt ist dies etwa bei *boost::function<>* schwierig.

Das Sortieren netzweit delegieren

Die Erstellung einer Client-Server-Applikation, in der der Server auf Anfrage eines Clients ein *secretContainer*-Objekt erzeugt, serialisiert und dem Client übermittelt, soll den Abschluss dieses Tutorials bilden. Der Client sortiert die Daten und schickt das Objekt an den Server zurück. Wichtig ist, dass die Kommunikation von den Clients ausgeht. Daher muss lediglich der Server eine öffentliche IP erhalten.

Listing 5: *secretContainer*-Klasse

```
class secretContainer
  :public base<shared_ptr<secretNumber> >
{
  ////////////////////////////////////////////////////////////////
  friend class boost::serialization::access;

  template<class Archive>
  void serialize(Archive & ar, const unsigned int version){
    using boost::serialization::make_nvp;
    ar & make_nvp("base", boost::serialization::base_object<
                         base<shared_ptr<secretNumber> > >(*this));
  }
  ////////////////////////////////////////////////////////////////
public:
  // Default constructor not shown. Initializes
  // random number generator
  // Initialize container with random numbers
  secretContainer(unsigned int size)
    :mersenne(static_cast<unsigned int> (time(0))),
     normalDist(0.,1.), gauss(mersenne,normalDist)
  {
    for(unsigned int i=0; i<size; i++){
      shared_ptr<secretNumber> p(new secretNumber(gauss()));
      this->push_back(p);
    }
  }
  string toString(void){
    ostringstream oss;  // serialize
    {
#ifdef XMLARCHIVE
      boost::archive::xml_oarchive oa(oss);
#else
      boost::archive::text_oarchive oa(oss);
#endif
      oa << boost::serialization::make_nvp("secretContainer",*this);
    } // archive and stream closed at end of scope
    return oss.str();
  }
  void fromString(const string& descr){
  { /* code analog toString() */ }

  virtual void sort(void){
    std::sort(this->begin(), this->end(),
      bind(&secretNumber::value,_1) < bind(&secretNumber::value,_2));
  }
private:
  mt19937 mersenne;
  normal_distribution<double> normalDist;
  variate_generator<mt19937&, normal_distribution<double> > gauss;
};
```

Listing 6: *main()*-Funktion

```
int main(int argc, char **argv){
  secretContainer sc(10);
  sc.sort();
  string serialization = sc.toString();
  // Let the user know
  cout << "Printing serialized secretContainer:" << endl;
  cout << serialization << endl;
  // Load serialized object into new secretContainer
  secretContainer sc2;
  sc2.fromString(serialization);
  cout << "Printing content of de-serialized secretContainer:" << endl
       << sc2 << endl;
  return 0;
}
```

```
Printing serialized secretContainer:
22 serialization::archive 4 0 0 0 0 0 0 10 1 0 1 4 1 0
0 -1.1783758763357466 4
/* 1-8 gelöscht */
9 1.1338391375353956
Printing content of de-serialized secretContainer:
-1.18 -0.65 -0.38 -0.20 0.32 0.45 0.55 0.63 1.00 1.13
```

Das reine Textarchiv von *Boost.Serialization* liefert kompakte Ergebnisse (Abb. 3).

Als Basis dient die *Boost.Asio*-Bibliothek. Diese ist noch nicht Teil der aktuellen Release 1.34.1, jedoch schon offiziell in die Boost-Familie aufgenommen worden. Ab Boost 1.35.x dürfte sie in der Kernbibliothek zu finden sein. Teil 2 des Tutorials ist bereits darauf eingegangen, wie man diese Bibliothek in Boost 1.34.1 einbaut.

Listing 7: *main()* für Client und Server

```
int main(int argc, char* argv[]){
  try {
    // Are we a client or a server ?
    if(argv[1] == string("client")){
      if (argc != 4) {
     std::cerr << "Usage: vectorExample client <host> <port>" <<
                                                          endl;
     return 1;
      }

      client Client(argv[2], argv[3]);
      Client.run();
    }
    else{
      if (argc != 3) {
     std::cerr << "Usage: vectorExample server <port>" << endl;
     return 1;
      }

      server Server(argv[2]);
      Server.run();
    }
  }
  catch (std::exception& e) {
    std::cerr << "Exception: " << e.what() << endl;
    return 1;
  }
  return 0;
}
```

Listing 8: *client*-Klasse

```
class client
{
public:
  client(string server, string port)
    :socket_(io_service_),
     resolver_(io_service_),
     query_(server, port)
  { endpoint_iterator0=resolver_.resolve(query_); }
  void run(void) {
    for(unsigned int i=0; i<NPROCESS; i++){
      if(!tryConnect()) {
        cout << "Error: Could not connect to server" << endl;
        break;
      }
      string data=retrieve();

      if(data == "error"){
        cout << "Error: Invalid response from server" << endl;
        break;
      }
      // De-serialize the object
      secretContainer sc;
      sc.fromString(data);
      // Sort it. This is where the actual work is done
      sc.sort();
      if(!tryConnect()) {
        cout << "Error: Could not connect to server" << endl;
        break;
      }
      // And send it off again
      submit(sc.toString());
      cout << "Processed one data set" << endl;
    }
  }
private:
  bool tryConnect(void){ /* See listing 9 for the code */ }
  string retrieve(void){ /* See listing 10 for the code */ }
  void submit(string data){ /* See listing 11 for the code */ }
  asio::io_service io_service_;
  socket socket_;
  resolver resolver_;
  resolver::query query_;
  resolver::iterator endpoint_iterator0;
  resolver::iterator end;
};
```

Es geht los mit dem stark vereinfachten Beispiel einer *main()*-Funktion, die sowohl für Clients als auch den Server verwendet wird (Listing 7). Zahl und Art der Argumente entscheiden über die Verwendung.

Sowohl die *server*- als auch die *client*-Klasse besitzen eine *run()*-Funktion, deren Aufruf nach der Initialisierung erfolgt. In puncto Fehlerbehandlung beschränkt sich das Programm darauf, pauschal alle von *std::exception* abgeleiteten Ausnahmen in *main()* abzufangen und sich gegebenenfalls zu beenden.

Zunächst ein Blick auf die *client*-Klasse (Listing 8). Als private Datenelemente existieren vier Objekte. *io_service* ist für das gesamte Low-Level-I/O-Management zuständig. Über das *socket*-Objekt erfolgt die Kommunikation, und ein *resolver*- sowie ein *query*-Objekt dienen der Namensauflösung.

Der Konstruktor initialisiert zunächst das *socket*- und anschließend das *resolver*- sowie das *query*-Objekt. Da es zu einer Kombination aus Hostname und Port verschiedene Auflösungen geben kann (man spricht vom „endpoint"), liefert *Boost.Asio* als Ergebnis eines *resolver.resolve()*-Aufrufs einen Iterator zurück, der alle möglichen Auflösungen durchlaufen kann. Den Endpunkt dieses Iterators, der in der *end*-Variable als privates Datenmember gespeichert wird, beschreibt der Default-Konstruktor. Da die Applikation mehrfach Verbindungen auf- und abbauen soll, speichert sie zudem das Ergebnis des *resolve()*-Aufrufs in *endpoint_iterator0*.

Statischer Setup vorausgesetzt

Es kann passieren, dass zwei *resolve()*-Aufrufe unterschiedliche Informationen zurückliefern – in diesem Fall wäre das Zwischenspeichern nicht sinnvoll. Für die vorliegende Spielzeug-Applikation soll jedoch von einem statischen Setup ausgegangen werden.

Als Nächstes ein Blick auf die *run()*-Funktion. Der Client soll sich *NPROCESS* mal mit dem Server verbinden, sich einen Vektor mit Zufallszahlen holen und diesen sortiert zurückschicken. Die Funktion *tryConnect()* baut zunächst eine Verbindung zum Server auf. Schlägt diese fehl, erfolgt eine Fehlermeldung und das Programm verlässt die *run()*-Schleife. Eine weitere Wrapper-Funktion – *retrieve()* – holt nun die Beschreibung eines *secretContainer*-Objekts vom Server. Hat der Server keine gültige Antwort geschickt, liefert *retrieve()* den String "*error*" zurück, was zur Beendigung der Schleife führt. War der Transfer erfolgreich, wird ein *secretContainer*-Objekt erzeugt. Der Aufruf von *secretContainer::fromString()* lädt die Objektbeschreibung in das *secretContainer*-Objekt. Am Ende der *retrieve()*-Funktion wird die Verbindung zum Server unterbrochen – hierzu unten mehr.

secretContainer::sort() erledigt die eigentliche Arbeit – das Sortieren des Vektors. Nun bleibt nur, das sortierte Objekt zum Server zurückzuschicken. Hierzu erfolgt wieder ein Verbindungsaufbau, *toString()* serialisiert den *secretContainer* und die Wrapper-Funktion *client::submit()* schickt die Daten zum Server zurück. Auch hier wird am Ende von *submit()* die Verbindung unterbrochen. Diese Unterbrechung für die Dauer der Berechnung ist sinnvoll, denn es ist für den Client nicht ersichtlich, wie lange dieser Vorgang dauert, da das nur dem *secretContainer*-Objekt bekannt ist.

Verbindung wieder aufnehmen

Die Funktion *client::tryConnect* (Listing 9) iteriert über alle Endpunkte. Das Ende der Iteration zeigt die bereits besprochene *end*-Variable an. Zunächst wird sicherheitshalber der *socket* geschlossen, danach erfolgt ein Verbindungsversuch zum Server über einen neuen Endpunkt. Ist dieser erfolgreich, setzt das Programm die Fehlervariable *error* auf *0*, und die *while()*-Schleife bricht ab. Nach dem Durchlaufen aller Endpunkte des *resolve()*-Aufrufs, ohne dass eine Verbindung zustande gekommen ist, erfolgt ebenfalls ein Programmabbruch. In diesem Fall ist *error* noch auf den Fehlercode *host_not_found* gesetzt. In diesem Fall liefert das Beispiel *false* als Ergebnis von *tryConnect()* zurück. Ist diese Hürde überwunden, war der Verbindungsversuch erfolgreich und der Rückgabewert ist *true*.

Nun kann es an den Empfang der Daten gehen (Listing 10). Die Funktion *client::retrieve()* schickt dem Server mithilfe von *asio::write()* über den in *tryConnect()* geöffneten Socket zunächst die Mitteilung *getData*. Diese teilt dem Server mit, dass sie ein neues

Datenpaket benötigt. Die Hilfsfunktion *commandString* erzeugt dabei einen String der Länge *COMMANDLENGTH*. Diese Länge ist mit dem Server fest vereinbart, da er keine Möglichkeit hat, diese Größe zur Laufzeit festzustellen.

Warten auf die richtige Antwort

Das Programm wartet nun auf eine Antwort des Servers. Die einzige zulässige Antwort auf *getData* ist das Kommando *compute*. Es liest die Antwort mithilfe von *asio::read()* über den Socket in ein Char-Array, das ebenfalls die Länge *COMMANDLENGTH* besitzt. Da die Antwort wahrscheinlich eine Reihe von Leerzeichen beinhaltet, entfernt die Boost-Funktion *trim_copy()* sie. Ist die erhaltene Antwort ungültig, schließt die Applikation den Socket und liefert den String "*error*" zurück.

Da bei der Programmierung des Beispiels ein Protokoll für den Datenaustausch zugrunde gelegt wurde, ist klar, dass nach dem *compute*-Kommando als nächstes Element die Größe der Datensektion – das heißt des serialisierten *secretContainer* – zu erwarten ist. Diese liest der Client ebenfalls in ein Char-Array passender Größe, entfernt die Leerzeichen und wandelt es mit *boost::lexical_cast<unsigned int>* in eine Variable um.

Nun wird ein *vector<char>* passender Größe für das serialisierte Objekt erzeugt, in den *asio::read()* die Daten des *secretContainer* einliest. Den in einen String gewandelten Vektor liefert der Client nach dem Schließen der Verbindung als Ergebnis der Operation zur weiteren Verarbeitung zurück.

Nach dieser Vorarbeit sollte der Inhalt der *submit()*-Funktion (Listing 11) sofort verständlich sein. Ihr Aufruf erfolgt nach getaner Arbeit und dient dazu, das Ergebnis der Berechnung an den Server zurückzuschicken. Hierzu schickt sie dem Server die Mitteilung *result*, gefolgt von der Größe des Datensegments und den Daten. Letztendlich bricht das Schließen des Socket die Verbindung ab.

Es bleibt noch die Erläuterung des Server-Codes: *server* ist die Management-Instanz, und *session* wird für jede neue Verbindung instantiiert. Zunächst zur *server*-Klasse (Listing 12). Als private Datenmember besitzt die *server*-Klasse ein *io_service*- sowie ein *acceptor*-Objekt. Letzteres ist für das Handling neuer Verbindungen zuständig und wird im Konstruktor mit Port und *io_service*-Objekt initialisiert. Ferner wird ein *threadpool*-Objekt mit vier Threads erzeugt. Das ist für das Funktionieren des Beispiels zwar nicht notwendig, kann die Klasse in ihrer Funktionsweise aber deutlich verbessern.

Der Konstruktor erzeugt ein neues *session*-Objekt in einem *shared_ptr*. Seine Verwendung erspart ein hässliches *delete this* im *session*-Objekt.

Das *acceptor*-Objekt wird angewiesen, eine neue Verbindung auf dem Socket des *session*-Objekts anzunehmen. *async_accept* erwartet neben dem Socket einen Handler für eine Funktion, deren Aufruf nach Beendigung der *accept*-Operation erfolgt. Sie erhält als einzigen Parameter einen Fehlercode. Nun sollen aber genau aus diesem Handler heraus neue *accept()*-Operationen und die dazugehörige Session starten, was die Übergabe weiterer Parameter erfordert. Hier hilft wieder *boost::bind()*, das eine *shared_ptr<session>* an das erste Argument von *server::handle_accept()* bindet. Der einzige freie Parameter dieser Funktion ist danach der Fehlercode. *asio::placeholders::error* fungiert einfach als Platzhalter für das *boost::bind*-typische *_1*.

Verbindung erfolgt im Hintergrund

Als asynchrone Operation beendet sich *async_accept* sofort nach dem Aufruf. Das Handling der neuen Verbindung findet im Hintergrund statt. Somit ist auch der Konstruktor beendet. In der *main()*-Funktion erfolgt nun der Aufruf von *server::run()*, was das *io_service*-Objekt veranlasst, die *event-loop* zu starten. Erst ab diesem Moment ist die Applikation wirklich einsatzfähig und in der Lage, neue Verbindungen anzunehmen.

Diese initiiert jeweils die *server::handle_accept()*-Funktion, die praktisch als Kopie des Konstruktors fungiert. Der einzige Unterschied zum Konstruktor ist, dass sie die aktuelle Session *current_session* dazu bewegt, ihre Arbeit zu tun. Im vorliegenden Fall bedeutet das, einem Client einen unsortierten Vektor zu liefern oder sortierte Vektoren anzunehmen.

Die Verlagerung dieser Arbeit in einen Thread würde das Beispiel noch

Listing 9: *tryConnect()*-Funktion

```
bool client::tryConnect(void){
      resolver::iterator endpoint_iterator=endpoint_iterator0;
      boost::system::error_code error =
           asio::error::host_not_found;
      while (error && endpoint_iterator != end){
           socket_.close();
           socket_.connect(*endpoint_iterator++, error);
      }
      if (error) return false;
      return true;
  }
```

Listing 10: *retrieve()*-Funktion

```
string client::retrieve(void){
    asio::write(socket_, asio::buffer(commandString("getData",
          COMMANDLENGTH)));
    char  inboundCommand_[COMMANDLENGTH];
    asio::read(socket_, asio::buffer(inboundCommand_));
    string inboundCommand=boost::algorithm::trim_copy(
          std::string(inboundCommand_, COMMANDLENGTH));
    if(inboundCommand != "compute") {
      socket_.close();
      return string("error");
    }
    char inboundHeader_[COMMANDLENGTH];
    asio::read(socket_, asio::buffer(inboundHeader_));
    string inboundHeader=boost::algorithm::trim_copy(
          std::string(inboundHeader_, COMMANDLENGTH));
    unsigned int dataSize = lexical_cast<unsigned int>
    (inboundHeader);
    vector<char> inboundData(dataSize);
    asio::read(socket_, asio::buffer(inboundData));
    ostringstream oss;
    vector<char>::iterator it;
    for(it=inboundData.begin(); it!=inboundData.end(); ++it)
          oss << *it;
    socket_.close();
    return oss.str();
  }
```

Listing 11: *submit()-Funktion*

```
void client::submit(string data){
    std::vector<asio::const_buffer> buffers;
    string result = commandString("result", COMMANDLENGTH);
    buffers.push_back(asio::buffer(result));
    string dataSize = commandString(lexical_cast<string>
         (data.size()),

COMMANDLENGTH);
    buffers.push_back(asio::buffer(dataSize));
    buffers.push_back(asio::buffer(data));
    asio::write(socket_, buffers);
    socket_.close();
  }
```

interessanter machen. Die hierfür notwendigen Änderungen sind überraschend klein. Verwendet man die in Teil 2 des Tutorials angesprochene *threadpool*-Bibliothek (deren Initialisierung bereits im Konstruktor erfolgt ist), muss man die *session::processRequest()*-Funktion lediglich als neue Task übergeben. Wird einer der vier konfigurierten Threads frei, beginnt er mit der Ausführung dieser Funktion, die bis zu diesem Zeitpunkt in einer Taskqueue gespeichert ist.

Listing 12: *server*-Klasse

```
class server{
public:
  server(string port)
    : acceptor_(io_service_, tcp::endpoint(tcp::v4(), lexical_cast<short>(port))),
      tp(4)
  {
    shared_ptr<session> new_session(new session(io_service_));
    acceptor_.async_accept(new_session->socket(),
          boost::bind(&server::handle_accept, this, new_session,
                           asio::placeholders::error));
  }
  void handle_accept(shared_ptr<session> current_session,
                           const boost::system::error_code& error) {
    if (error) return;
    // You need to comment-out "current_session->processRequest();" below,
    // if you want to use this.
    // tp.schedule(boost::bind(&session::processRequest,current_session));
    // Make sure a new session is started before we handle the current request
    shared_ptr<session> new_session(new session(io_service_));
    acceptor_.async_accept(new_session->socket(),
                           boost::bind(&server::handle_accept, this, new_session,
                           asio::placeholders::error));
    current_session->processRequest();
  }
  void run(void){
    io_service_.run();
  }
private:
  asio::io_service io_service_;
  tcp::acceptor acceptor_;
  boost::threadpool::pool tp;
};
```

Listing 13: *session*-Klasse

```
class session
{
public:
  session(asio::io_service& io_service)
    : socket_(io_service)
  { /* nothing */ }
  tcp::socket& socket() { return socket_; }

  void processRequest() {
    // First check what the client wants from us.
   // This will remove the command from the stream.
    char  inboundCommand_[COMMANDLENGTH];
    asio::read(socket_, asio::buffer(inboundCommand_));
    string inboundCommand=boost::algorithm::trim_copy(
                         std::string(inboundCommand_, COMMANDLENGTH));
    // We accept only two commands: "getData" and "result"
    if(inboundCommand == "getData"){
      // Create a new secretContainer object, serialize it and send it off
      cout << "Received getData command" << endl;
      secretContainer sc(VECTORSIZE);
      submit(sc.toString());
      cout << "Sent off data" << endl;
    }
    else if(inboundCommand == "result"){
      // De-serialize the data and print the resulting object
      cout << "De-serializing data" << endl;
      string data=retrieve();
      secretContainer sc;
      sc.fromString(data);
      cout << "Received a response" << endl;
    }
    else{
      cout << "Error: unknown command: " << inboundCommand << endl;
      return;
    }
  }
private:
  void submit(string data){ /* see listing service */ }
  string retrieve(void){ /* see listing service */ }

  tcp::socket socket_;
};
```

Allerdings muss man sich sicher sein, dass *processRequest()* auch für die Ausführung in einer Multithreaded-Umgebung geeignet ist. Und genau hier gibt es bei *Boost.Serialization* im Moment Fragezeichen. Eine neue, sicherere Version dieser Bibliothek ist aber unterwegs. Gleichwohl ist die betreffende Zeile der *handle_accept()*-Funktion deshalb auskommentiert. Die Verwendung von *Boost.Serialization* mit *Boost.Asio* allein scheint trotz dessen asynchronen Designs aber sicher zu sein.

Wichtig sind noch zwei Bemerkungen: Beim momentanen Design startet der Server auf dem Umweg über *handle_accept* in jeder *async_accept()*-Operation eine neue Aktion. Dies führt zwar zu einer Endlosschleife, überschwemmt den Rechner aber nicht mit *async_accept*-Operationen. Denn ein weiterer *async_accept*-Aufruf erfolgt erst, wenn ein Client eine neue Verbindung akzeptiert. Die Zahl der *accept*-Aufrufe entspricht also immer der benötigten Zahl.

Den Einbau eines Mechanismus zur Beendigung des Servers berücksichtigt das Beispiel nicht. Hierfür müsste man einfach auf die Annahme weiterer Verbindungen verzichten, indem kein weiterer *async_accept*-Aufruf erfolgt. In dem Fall würde sich *io_service.run()* beenden.

Ein Blick auf die *session*-Klasse (Listings 13) soll das Tutorial abschließen. Jedes *session*-Objekt erhält seinen eigenen Socket – er wird im Konstruktor mithilfe einer Referenz auf den *io_service* initialisiert. Die eigentliche Arbeit übernimmt *session::processRequest()*.

Wie beim Client liest die Funktion zunächst die Mitteilung der Gegenseite. Zwei Kommandos sind erlaubt: *getData* und *result*. Der erste Fall erzeugt einen unsortierten *secretContainer* der Größe *VECTORSIZE*, serialisiert ihn und schickt ihn über die Hilfsfunktion *session::submit()* zum Client.

Im zweiten Fall empfängt *session::retrieve()* die Antwort (insbesondere den sortierten Vektor) und lädt die Daten zurück in einen *secretContainer*.

Die Zerstörung des *session*-Objekts impliziert das Schließen des Socket. Dies geschieht, wenn die letzte Kopie des *shared_ptr<session>* für das aktuelle *session*-Objekt in der *server*-Klasse seinen Geltungsbereich verlässt. *session::submit()* und *session::retrieve()* folgen dem aus der *client*-Klasse bekannten Schema. (ka)

DR. RÜDIGER BERLICH

führt am Institut für Wissenschaftliches Rechnen des Karlsruhe Institute of Technology (KIT) eine Ausgründung aus dem Bereich der Parameteroptimierung in verteilten Umgebungen durch.

Tutorialinhalt

Teil I: Allgemeine Eigenschaften, Shared Pointer und Container-Klassen, Operatoren, Lizenzmodell

Teil II: Speicherung von Funktionszeigern und Objekten, Thread-Programmierung, Umgang mit Zeit-Ausdrücken

Teil III: Zufallszahlen, Serialisierung und Netzwerkprogrammierung

Onlinequellen

[a] Boost Random Number Library
www.boost.org/libs/random/index.html

[b] Class Serialization Traits
www.boost.org/libs/serialization/doc/traits.html

[c] Serialization: Special Considerations
www.boost.org/libs/serialization/doc/special.html

JPEG-Dateien mit ImageMagick kacheln

Bildersturm

Henning Behme

Wer Fotos vor der Webveröffentlichung bearbeiten oder nur Ausschnitte bringen will, dem steht jede Menge Software zur Verfügung. Dazu zählt ImageMagick, das sich unter anderem zur Batch-Verarbeitung eignet.

Bilder ins Web zu stellen, ist mittlerweile eine Volkssportart. Michael Riepe hat schon in *iX* 7/07 gezeigt, welche Hilfe die *netpbm*-Tools dabei sein können. Das ImageMagick-Paket bietet mit mehreren Teilprogrammen (*convert*, *montage*, ...) ebenfalls Unterstützung auf der Kommandozeile – etwa für Batch-Verarbeitung. Hier sei ein Shellskript vorgestellt, das eine JPEG-Datei in eine im Prinzip beliebige Anzahl von Kacheln zerteilt.

Listing 1: tileimg

```
#!/bin/bash

FILE=$1
BANZAHL=${2:-1}
HANZAHL=${3:-1}
FORMAT=${4:-jpg}

geometrie() {
  BREITE=$1
  HOEHE=$2
}

### Bildbreite und -hoehe eruieren
geometrie `djpeg -pnm  ${FILE}.${FORMAT} | sed -ne 2p`

### Variablen initialisieren
X=0
Y=0
i=1
BSTREIFEN=$(((BREITE + BANZAHL-1) / BANZAHL))
HSTREIFEN=$(((HOEHE + HANZAHL-1) / HANZAHL))

### Aeussere und innere Schleife fuer Kacheln
while [ $X -lt $BREITE ]
do
  cp $FILE.$FORMAT $FILE$i.$FORMAT
  mogrify -crop ${BSTREIFEN}x${HOEHE}+${X}+${Y} $FILE$i.$FORMAT
  j=1
  while [ $Y -lt $HOEHE ]
  do
    cp $FILE$i.$FORMAT $FILE$i$j.$FORMAT
    mogrify -crop ${BSTREIFEN}x${HSTREIFEN}+0+${Y} \
         $FILE$i$j.$FORMAT
    Y=$((Y+HSTREIFEN))
    j=$((j+1))
  done
  X=$((X+BSTREIFEN))
  i=$((i+1))
  Y=0
done
```

Um ein Bild modifizieren zu können, muss der Bearbeiter ein Programm zur Verfügung haben, das „weiß“, welches Format das ihm übergebene Bild hat und wie viele Kacheln als Ergebnis herauskommen sollen. Deshalb erhält das nebenstehende *tileimg* zunächst Parameter, die es Variablen zuweist, wobei die vierte optional ist – nur erforderlich, wenn es sich nicht um JPEG-Daten handelt (*djpeg* soll zwar nur JPG auspacken, aber ein Versuch mit PNG zeigte dasselbe Ergebnis).

Ein Aufruf von *djpeg* und die Umleitung seiner Ausgabe nach *sed* bewirken, dass die Shellskriptfunktion *geometrie* aus dem Originalbild zunächst die Breite und Höhe übergeben bekommt. Die *sed*-Optionen *–ne* bedeuten „Input-Zeile nicht ausgeben“ (*n*) und „folgendes Kommando ausführen“ (*e*). *2p* veranlasst *sed*, die zweite Zeile auszugeben.

Zwei Schleifen, sie alle zu kacheln

Was das Skript außerdem „wissen“ muss: in wie viele Streifen die Vorlage waagerecht und senkrecht aufzuteilen ist. *BSTREIFEN=$(((BREITE + BANZAHL - 1) / BANZAHL))* hat zum Ergebnis eine ganze Zahl, die nicht kleiner ist als der Quotient aus *BREITE* und *BANZAHL*. Analoges gilt für *HSTREIFEN*.

mogrify, Bestandteil des ImageMagick-Pakets, beschneidet Bilddateien. Aus einem Bild der Größe 1229 × 922 etwa ergäbe

```
mogrify –crop 410x308+410+308 datei
```

bei drei Kacheln in Höhe und Breite die mittlere (= zweite der zweiten Reihe).

Zwei Arbeitsschritte muss *tileimg* ausführen, damit nach dem Programmlauf alle Kacheln erzeugt sind. Im ersten transformiert das Skript Kopien der Originaldatei in drei senkrechte Balken von der errechneten Breite. Im zweiten Schritt, jeweils Bestandteil des ersten, geht es darum, aus dem gerade erstellten Balken drei in der Senkrechten geteilte Kacheln zu extrahieren.

Zwei *while*-Schleifen setzen das um. Die äußere kopiert in jedem Durchlauf (solange *X* kleiner als die Gesamtbreite ist) das Original in die Streifen-Datei, um Letztere anschließend mit *mogrify* zu modifizieren. Die Option *crop* bewirkt gleichsam ein Ausschneiden des angegebenen Bildteils, wie oben zu sehen.

Innerhalb dieses Durchgangs, wenn *mogrify* aus der Gesamtkopie einen Balken transformiert hat, kopiert das Skript ihn in der inneren *while*-Schleife in die Datei, die die jeweilige Kachel enthalten soll und wendet erneut *mogrify* an (solange *Y* kleiner als die Bildhöhe ist). Wichtig: In der inneren Schleife muss der *X*-Offset immer den Wert 0 haben, während er in der äußeren nach jedem Durchlauf erhöht wird. Analog gilt für *Y*, dass es am Ende der äußeren Schleife wieder auf 0 zu setzen ist, damit die beim nächsten Durchgang wieder den Ausgangswert vorfindet. Was im Listing fehlt ist, überflüssige Dateien zu löschen.

Dem Webauteur nicht zu schweur

Was das nebenstehende Skript nicht leistet: die Generierung des erforderlichen HTML-Codes. Da müssen Webautoren ran und per *div*, *p* oder *table* die gewünschten Kacheln mit dem gewünschten Stil (*visibility: hidden/visible*) versehen, den man wiederum per Javascript beim Mouseover oder dergleichen verändern kann.

Für diejenigen, die die notwendigen Tools nicht auf ihrem Rechner haben, steht ImageMagick unter www.imagemagick.org für diverse Systeme zum Download bereit. *djpeg* und *sed* sind auf Linux-Systemen und Mac OS X vorhandene Unix-Werkzeuge, die unter Umständen per *apt-get* oder einem ähnlichen Kommando nachzuinstallieren sind. (hb)

Mitarbeit am Skript: Michael Riepe

Zahlen- und Stellenwertsysteme

Eins, 2, III

Kai König

Das kleine Einmaleins lernen Kinder in der Grundschule. Die Zahlen des Dezimalsystems, die allen von klein auf vertraut sind, gelten in der westlichen Welt fast als Naturgesetz. Dabei kann man auch ganz anders zählen.

Stoff für Ausflüge in das Reich der Mathematik gibt es genug – siehe beispielsweise den Internet-Infos-Beitrag aus dem Jahr 2006 (www.heise.de/ix/artikel/2006/05/162/). Im heutigen Artikel geht es um Zahlen- und Stellenwertsysteme.

Zunächst der Versuch einer Definition und Abgrenzung beider Begriffe. Ein Zahlensystem dient der Darstellung abstrakter mathematischer Objekte, die zum Zählen, Ordnen und Messen verwendet werden (de.wikipedia.org/wiki/Zahl), und beschreibt Regeln für Ziffern sowie deren Verwendung zur Bildung von Zahlen. Den Begriff Stellenwertystem verwenden Mathematiker, wenn sie von einem bestimmten Typ Zahlensystem sprechen, der die Wertigkeit einer Ziffer anhand ihrer Stelle in der Notation der Zahl definiert. Ein anderer Begriff für Stellenwertsystem ist Positionssystem. Dessen bekanntester Vertreter ist sicherlich das im Alltag vielfach verwendete Dezimalsystem mit den Ziffern 0 bis 9 (www.itwissen.info/definition/lexikon/__place%20value%20system_stellenwertsystem.html). In der Informatik sind Stellenwertsysteme mit anderen Basen als das Binärsystem (Basis 2 mit den Ziffern 0 und 1), das Oktalsystem zur Basis 8 sowie das Hexadezimalsystem zur Basis 16 (mit den Ziffern 0 bis 9 sowie A bis F) gebräuchlich.

Als anderen Haupttyp von Zahlensystemen versteht man die Additionssysteme (de.wikipedia.org/wiki/Additionssystem). Sie beschreiben den Wert einer Zahl durch Addieren der Werte ihrer Ziffern. Ein bekanntes Beispiel sind die römischen Zahlen mit den sieben Ziffern I (1), V (5), X (10), L (50), C (100), D (500) und M (1000). In diesem System gibt es allerdings die Besonderheit der subtraktiven Schreibweise: Die Ziffern I, X und C dürfen einer der beiden jeweils nächsthöheren Ziffern vorangestellt und vom Wert der höheren Ziffern abgezogen werden, etwa IV für vier oder XC für 90. Die subtraktive Schreibweise ist erstaunlicherweise erst seit dem späten Mittelalter regelmäßig in Erscheinung getreten und belegt somit, dass sich auch Zahlensysteme im Laufe der Zeit verändern können. Der Wikipedia-Artikel zu den römischen Zahlen geht auf Rechenregeln und verschiedene Schreibweisen für sehr große Zahlen im römischen Additionssystem ein (de.wikipedia.org/wiki/R%C3%B6mische_Zahlen). Eine praktische Anwendung findet sich unter der URL www.uhrenhanse.de/sammlerecke/wissenswertes/hoffmann.htm. Eine Abhandlung geht hier der Frage nach der korrekten Verwendung der römischen Schreibweise der Zahl Vier auf analogen Zifferblättern von Uhren nach.

Schnell umgerechnet

Ebenfalls einen Blick wert sind On- und Offline-Werkzeuge zur Umrechnung zwischen den römischen Zahlen und dem Dezimalsystem. Netzreport (netzreport.googlepages.com/online_umrechner_fuer_dez_roemzahl.html) stellt neben einem solchen Javascript-basierten Umrechner diverse Werkzeuge für die Konvertierung zwischen verschiedenen Stellenwertsystemem bereit (netzreport.googlepages.com/online_umrechner_fuer_zahlensysteme.html). Die Offline-Alternative für Mac-Benutzer ist ein Dashboard Widget namens *NumericRoman* (www.apple.com/downloads/dashboard/calculate_convert/numericroman.html).

Wer sich ein wenig für die mathematischen Hintergründe der Umrechnung interessiert, ist bei Arndt Brünner gut aufgehoben (www.arndt-bruenner.de/mathe/scripts/Zahlensysteme.htm#txthorner). Neben Informationen und Erläuterungen zur Sekundarstufen-Mathematik findet man dort Instruktionen zur schrittweisen Umrechnung anderer Stellenwertsysteme ins Dezimalsystem mit dem Hornerschema.

Heutzutage ist es nahezu selbstverständlich, Ziffern und Zahlen in verschiedenen Systemen zur Verfügung zu haben. Aber wie rechenhilfsmittel.de zeigt, war dies noch vor nicht allzu langer Zeit keine Selbstverständlichkeit. Das Kapitel „Entwicklung der Zahlensysteme“ (www.rechenhilfsmittel.de/zahlen.htm) erläutert den Ursprung der Zahlensysteme, indem es untersucht, wie sich das abstrakte Konzept entwickelt hat und es zur Trennung von der Zahl und den zu zählenden Dingen kam.

Viele Zahlensysteme beruhen auf einer natürlichen Gliederung (5 Finger einer Hand, 10 Finger beider Hände oder 20 Finger und Zehen). Das erste System der griechischen Zahlendarstellung basierte beispielsweise auf dem sogenannten akrophonen Prinzip, das heißt, der erste phonetische Buchstabe einer Ziffer diente als deren Symbol.

Eine Ausnahme von der natürlichen Gliederung waren die auf der Zahl 60 basierenden Zahlensysteme der Sumerer und Babylonier (www.8bit-museum.de/docs/history1.htm). Erklärt wird dies mit der vergleichsweise hoch entwickelten Astronomie dieser Kulturen – letztlich hat ein Nachfahre dieser 60er-Einteilung in Form der Unterteilung einer Stunde in 60 Minuten beziehungsweise 60 × 60 Sekunden überlebt.

Der Artikel „Mathematik durch die Jahrtausende“ (www.mathematik.de/mde/information/matheInGeschichteUndGegenwart/jahrtausende/jahrtausende.html) liefert einen guten Überblick über die Anfänge der Mathematik und die Besonderheiten der Lehre von den Zahlen in verschiedenen Kulturkreisen. Hier erfährt man beispielsweise, dass die frühe chinesische Mathematik auf Zähltafeln beruhte und somit bereits circa 400 v. Chr. praktische Aufgaben wie die Landvermessung et cetera in einem Dezimalsystem gelöst wurden. Wer hingegen demnächst privat oder beruflich nach China muss, ist vielleicht eher an der Kurzeinführung in das Zählen mit der Hand interessiert: www.stabi.hs-bremerhaven.de/dss/Zahl.html. Als Abschluss des Ausflugs in die

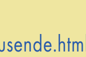
Geschichte noch ein weiteres Umrechnungs-Tool von der Dezimalschreibweise ins Zahlensystem der Maya: fliegen123.fl.funpic.de.

Die heute so geläufigen Symbole, oftmals arabische Zahlen genannt, stammen eigentlich aus Indien und haben ihren Weg über Asien und Spanien in die westliche Welt gefunden. Mit dem Dezimalsystem ist die Entwicklung aber noch nicht abgeschlossen. Auf seiner Homepage stellt Leonhard Heinzmann alternative Zahlensysteme vor und führt in das Rechnen mit ihnen ein. Interessant ist sein Konzept der sogenannten Plus-Zahlensysteme, das speziell in Form des 3+1-Systems relativ detailliert ausgearbeitet ist (members.aol.com/leonheinz/dreiplus1-system.htm). Herr Heinzmann widmet sich auch der Frage, welches Zahlensystem für den Menschen am besten nutzbar ist, und kommt zu dem Schluss, dass es sich dabei um das Vierersystem handele (also einem Stellenwertsystem mit der Basis 4 und den Ziffern 0 bis 3). Eine ähnliche Untersuchung führt Werner Brefeld (www.brefeld.homepage.t-online.de/zahlensysteme.html) durch, kommt allerdings zu einem abweichenden Ergebnis und hält das 6er-, das 10er- und das 16er-System für am geeignetsten. Grundlage dieser Untersuchung sind im Wesentlichen einfache Regeln für die Teilbarkeit. Wie so oft gibt es keine eindeutige Antwort – angesichts der tiefen Verwurzelung des Dezimalsystems im westlichen Kulturkreis hat diese Diskussion aber ohnehin eher akademischen Charakter. (ka)

URLs auf einen Blick

www.heise.de/ix/artikel/2006/05/162/
de.wikipedia.org/wiki/Zahl
www.itwissen.info/definition/lexikon/__place%20value%20system_stellenwertsystem.html
de.wikipedia.org/wiki/Additionssystem
de.wikipedia.org/wiki/R%C3%B6mische_Zahlen
www.uhrenhanse.de/sammlerecke/wissenswertes/hoffmann.htm
netzreport.googlepages.com/online_umrechner_fuer_dez_roemzahl.html
netzreport.googlepages.com/online_umrechner_fuer_zahlensysteme.html
www.apple.com/downloads/dashboard/calculate_convert/numericroman.html
www.arndt-bruenner.de/mathe/scripts/Zahlensysteme.htm#txthorner
www.rechenhilfsmittel.de/zahlen.htm
www.8bit-museum.de/docs/history1.htm
www.mathematik.de/mde/information/matheInGeschichteUndGegenwart/jahrtausende/jahrtausende.html
www.stabi.hs-bremerhaven.de/dss/Zahl.html
fliegen123.fl.funpic.de
members.aol.com/leonheinz/dreiplus1-system.htm
www.brefeld.homepage.t-online.de/zahlensysteme.html

Wer weitere URLs zum Thema kennt, hat die Möglichkeit, sie der Online-Version (www.heise.de/ix/artikel/2008/02/146/) hinzuzufügen.





Vor 10 Jahren: Kein Vitamin CCC für DIRC

Auf dem Jahreskongress 1998 des Chaos Computer Clubs machte ein „Netzwerk ohne Carrier“ Furore.

Seit 24 Jahren tagt der Chaos Computer Club (CCC) zwischen Weihnachten und Silvester. Vor 10 Jahren standen bereits Themen wie Datenschutz, Kryptografie und Steganografie sowie Wirtschaftsspionage durch Hacker im Internet auf der Tagesordnung. Und weil damals Innenminister Kanther das Internet und die Telekommunikation regulieren wollte, war das Interesse an alternativen Vernetzungssystemen groß.

Einer der Höhepunkte auf dem Hackerkongress war darum eine durchaus kommerzielle Produktvorstellung, über die *iX* 2/1998 unter dem Titel „DIRC-Netzwerk ohne Carrier“ berichtete. DIRC, ausgeschrieben „Digital Inter Relay Communication“, wurde als völlig neue Kommunikationstechnologie angepriesen. Technisch sollte das Kommunikationsnetz aus Endgeräten für den Telefon- und Datenverkehr bestehen, die ihrerseits mit drei bis acht Nachbarstationen im maximalen Abstand von 5 Kilometern drahtlos permanent verbunden sind und die Kommunikation routen. Zumindest die Großstädte sollten mit DIRC-Stationen gut versorgt werden, für eine Monatspauschale von 50 DM. Kein Wunder, dass die Datenreisenden noch auf dem Kongress die DIRC-Prototypen kaufen wollten und von einer alternativen, fast kostenlosen Vernetzung schwärmten.

Doch das von der Firma Cetecom angeschobene Projekt hatte mit Finanzierungsengpässen zu kämpfen. Erst auf der Cebit 2000 konnten die Vorserienmodelle präsentiert werden. Dann dauerte es noch einmal zwei Jahre, bis die neu gegründete DIRC Technologie in Ratingen bei Düsseldorf ein stadtweites Netz installieren konnte – mit komplett neuer Technik: inzwischen hatte sich WLAN nach 802.11b etabliert. Doch auch die Aufgabe der eigenen proprietären Technologie konnte DIRC nicht retten, weil Internetzugänge gerade in den großen Städten immer schneller wurden und sogar Voice over IP ermöglichten.

Heute ist DIRC verschwunden, die grundlegende Idee jedoch nicht. Sie wurde vom spanisch-argentinischen Investor Martin Varsavsky aufgegriffen, der mit seinem Moviemento Fonero die Welt mit „La Fonera“ genannten WLAN-Routern überziehen möchte. Das Geschäftsmodell basiert darauf, dass Foneros die Infrastruktur anderer Foneros kostenlos nutzen können, an ihrem Hotspot jedoch zusammen mit Fon auch Geld verdienen können. Obwohl auf Datenkommunikation ausgerichtet, ist auch VoIP in den Expansionsplänen zur Weltvernetzung der Foneros enthalten. Skype ist einer der Großinvestoren in das Schneeballsystem von Fon, das wie DIRC davon abhängig ist, möglichst schnell eine kritische Masse zu erreichen.

Richtige Hacker betrachten das Moviemento Fonero jedoch mit Skepsis. Sie bemängeln die proprietäre Technologie wie die Tatsache, dass die Hotspots prinzipiell nicht verschlüsseln können. Für sie ist Freifunk.net als basisdemokratische WLAN-Vernetzung der eigentliche Erbe einer Idee, unabhängige Kommunikationsnetze für jedermann von jedermann ohne Carrier-Kontrolle zu errichten. *Detlef Borchers*

MEHR KBYTES

Windows/WWW

Microsoft und das Web – das war anfangs eine Geschichte von Verschlafenheit auf Seiten der Redmonder. Die ist allerdings mehr als zehn Jahre her. Mittlerweile trachten MS-Entwickler danach, Teile der Funktionen, die sie innerhalb des Betriebssystems bieten, in den hauseigenen Browser Internet Explorer – mit Silverlight sogar darüber hinaus (Firefox, Safari) – zu integrieren.

Innerhalb neuerer Windows-Versionen ist die Windows Presentation Foundation (WPF) die Basis der grafischen Anwendungen. Chris Sells und Ian Griffiths haben bei O’Reilly 2007 die zweite Auflage ihres „Programming WPF“ veröffentlicht, das sich im Wesentlichen auf die Anwendungsentwicklung konzentriert, durch Einbeziehung der XAML Browser Applications (XBAPs) aber außerdem mit dem IE 6+ Darstellbares beinhaltet. Ein Silverlight-Tutorial ergänzt die Informationen zu XAML um Weborientiertes. Über 800 Seiten Lesestoff, eher für Windows-Entwickler mit Webneigung als für reine WWW-Programmierer.

Mit einem Windows-Server dürften fast alle Beteiligten statt Apache Microsofts IIS als Webserver nutzen. Bis Version 6 handelte es sich um eine monolithische Anwendung, aber IIS 7 ist modular angelegt, sodass Administratoren nur noch das einspielen und verwalten müssen, was sie benötigen. Chris Adams, selbst im IIS-Team tätig, hat mit seinen Koautoren zusammengetragen, worauf Webadmins beim Wechsel auf den neueren Server achten müssen: „How to Cheat at IIS 7 Server Administration“ bietet alles, was man wissen muss, um mit beliebigen Gesprächspartnern intelligent über den Server sprechen zu können – schreibt Adams selbst im Vorwort.

Um es sarkastisch auszudrücken: Es soll Webprofis geben, die ihre Sites mit Frontpage zu erstellen pflegten. Die haben mit dem 2007 fertiggestellten Nachfolgeprodukt Expression Web jetzt etwas Besseres (und weniger Rufschädigendes) zur Verfügung. Helma Spona führt bei Markt + Technik auf circa 400 Seiten in den Umgang mit diesem „fast perfekten Dreamweaver-Klon“ ein.

MS-Webentwickler dürften außer dem IIS als Grundlage meist mit ASP.Net arbeiten, um Webanwendungen zu erstellen. Scott Allen und vier weitere Autoren haben bei Sitepoint eine „ASP.NET 2.0 Anthology“ zusammengestellt, die einem Kochbuch ähnlich Tipps und Tricks verrät. Nach einführenden Kapiteln widmen die Autoren sich Themen wie Datenzugriff, Formularvalidierung, Komponenten, Ajax und E-Mail. Keine Rundum-Referenz, sondern ein Stöberwerk für Einsteiger und Fortgeschrittene.

Das erwähnte Ajax (Asynchronous Javascript and XML) ist im Grunde betriebssystemunabhängig. Will man diese Technik allerdings mit Microsofts ASP.Net verstärkt einsetzen, reicht die allgemeine Ajax-Einführung (oder das einzelne Kapitel wie oben) nicht, und spezielle Literatur muss her. Sie ist, wenig überraschend, reichlich vorhanden.

Dino Esposito hat im vorigen Jahr sein Werk zur ASP.Net-Ajax-Programmierung (das frühere Atlas-Projekt) veröffentlicht, das die Microsoft Press in einer deutschen Übersetzung anbietet. Auf gut 300 Seiten hat der Autor kompakt dargestellt, wie sich die Arbeit mit Microsofts Ajax-Ergänzung (per Javascript auf Client- und ASP.Net auf Serverseite) darstellt.

Auf ähnliche Weise geht Christian Wenz bei O’Reilly vor, dessen Band in deutscher Übersetzung von Lars Schulten gleichzeitig mit der US-Ausgabe erschienen ist. Ob Espositos oder Wenz’ Band die geeignetere Lektüre ist, zeigt erst ein genaues Studium der Ausführlichkeit einzelner Aspekte in Inhaltsverzeichnis.

O’Reilly hat in den USA mit „Learning ASP.NET 2.0 with Ajax“ einen weiteren Band im Programm, der in diese Microsoft-Technik einführt – ähnlich reich mit Listings versehen wie die beiden vorgenannten und explizit als Vorstufe zum Wenz’schen Werk gedacht.

2008 hat gerade begonnen, da liegt mit der 11. Auflage des Webadressbuchs für Deutschland das aus dem Hause Michael Weber stammende Internetverzeichnis für dieses Jahr schon vor. 6000 „wichtigste“ Adressen, zum Teil mit Screenshots beziehungsweise kurzen Erläuterungen versehen. Eine Redaktion wählt wie in der Vergangenheit aus den Anträgen aus, damit es bei den 6000 Sites bleibt. Da der Verlag zwei unterschiedliche kommerzielle Varianten des Eintrags vorsieht (99 respektive 599 € pro Jahr) müssen allerdings je nach deren Aufkommen die gemeinen kostenlosen 120-Zeichen-Einträge weichen. Thematisch geordnet und auf deutschsprachige Sites konzentriert, bietet der Band eine nichtrepräsentative Momentaufnahme, die 2008 mit einem Sonderteil zum Web 2.0 – Mitmach-Sites – beginnt.

Henning Behme

Chris Adams, Gene Whitley, Conrad Agramont; **How to Cheat at IIS 7 Server Administration**; Burlington, MA (Syngress/Elsevier) 2007; 377 Seiten; US-$ 49,95 (Paperback)

Scott Allen, Jeff Atwood, Wyatt Barnett, Jon Galloway, Phil Haack; **The ASP.NET 2.0 Anthology**; 101 Essential Tips, Tricks & Hacks; Collingwood, Australien (SitePoint) 2007; 572 Seiten; US-$ 39,95 (Paperback)

Dino Esposito; **ASP.NET AJAX Programmierung**; Eine Einführung in die Programmierung schneller und interaktiver Webanwendungen; München (Microsoft Press) 2007; übersetzt von Uwe Thiemann; 319 Seiten; € 39,90 (gebunden)

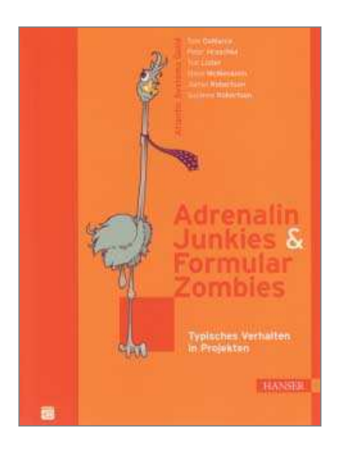
Jesse Liberty, Dan Hurwitz, Brian MacDonald; **Learning ASP.NET 2.0 with AJAX**; Sebastopol, CA (O’Reilly Media) 2007; 498 Seiten; € 43,– (Paperback)

Chris Sells, Ian Griffiths; **Programming WPF**; Building Windows UI with Windows Presentation Framework; Sebastopol, CA (O’Reilly Media) 2007; 2. Auflage; 835 Seiten; € 48,– (Paperback)

Helma Spona; **Microsoft Expression Web**; Der einfache Einstieg in die Webseitengestaltung; München (Markt + Technik) 2007; 409 Seiten; € 29,95 (Paperback)

Michael Weber (Hrsg.); **Das Web-Adressbuch für Deutschland 2008**; Die 6000 wichtigsten deutschen Internet-Adressen; Frankfurt/Main (M. W. Verlag) 2007; 11., völlig überarbeitete und aktualisierte Auflage 829 Seiten; € 16,90 (Paperback)

Christian Wenz; **Programmieren mit ASP.NET AJAX**; Köln (O’Reilly) 2007; übersetzt von Lars Schulten; 459 Seiten; € 44,90 (gebunden)



Tom DeMarco,
Peter Hruschka und andere

Adrenalin Junkies & Formular Zombies

Typisches Verhalten in Projekten

Übersetzt von Dirk Wittke
München, Wien 2007
Carl Hanser
220 Seiten
24,90 €
ISBN 978-3-446-41254-5

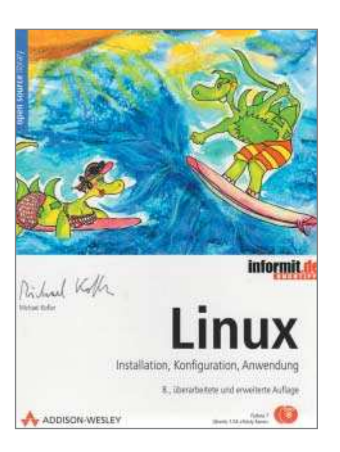
Wer Tom DeMarco kennt, weiß, womit der sich befasst. Und seine Mitstreiter der Atlantic System Guild sind in der Welt der Softwareentwicklung ebenfalls bekannte Größen. In ihrem neuen Buch befassen sich die sechs Autoren mit den weichen Faktoren, die schnell zu harten Fakten führen. Diese weichen Faktoren sind 86 Muster für typische Personen oder bekanntes Verhalten in IT-Projekten. Adrenalin-Junkies und Formular-Zombies sind zwei dieser Personentypen.

Obwohl die beiden Typen im Titel eine Konzentration auf negative Aspekte vermuten lassen, sind die beschriebenen Muster durchaus bunt gemischt. Der Leser profitiert hier von der Erfahrung aus Tausenden von Projekten, an denen die Autoren mitwirken konnten. Sie beschreiben unterschiedlichste Szenarien, mal mit fiktiven Personen, mal aus anonymisierten echten Projekten, die jedem mit eigener Erfahrung schnell bekannt vorkommen. Die geschilderten Menschenschläge und Aktivitäten finden sich immer wieder und führen in der Regel zum selben Ergebnis – positiv wie negativ. Und hier zeigt sich die Zielsetzung der Autoren. Der Leser soll für diese Muster und ihre Auswirkungen sensibilisiert werden, um sie schneller zu erkennen, Positives zu fördern und Negatives abzuwenden. Beides hilft, Projekte positiv abzuschließen und ein produktives Klima im Team zu schaffen.

Kapitelüberschriften sagen einiges aus, hier eine kleine Übersicht: „Toter Fisch“, „Management nach Gefühlslage“, „System Development Lemming Cycle“, „Bauchfrei steht nicht jedem“, „Feature-Suppe“, „Extreme Knigge“ und „Babylon“. Diese wenigen Titel erlauben schon einen Einblick in den Umfang, die Fantasie und die lockere Feder der Autoren. So ist beispielsweise das Kapitel „Filmkritiker“ eine schöne Beschreibung der Personen, die stets alles bewerten, aber nie selbst Verantwortung übernehmen. Diese Art Mensch dürfte vielen bekannt sein.

Der Band hält, was er verspricht. DeMarco und seinen Koautoren ist wieder ein humorvolles Fachbuch gelungen, etwas, das leider selten ist. Ihr Buch ist spannend, jedes Kapitel macht Lust auf mehr. Diese Autoren wissen, wie wichtig der Faktor Mensch in Projekten ist und können das sogar vermitteln.

FRANK MÜLLER



Michael Kofler

Linux

8., überarbeitete und erweiterte Auflage
München 2007
Addison-Wesley
1339 Seiten
59,95 €
ISBN 978-3-8273-2478-8

Immer mehr Leute setzen Linux ein – und wissen immer weniger darüber. Hilfe bietet da ein Buch wie „Linux. Installation, Konfiguration, Anwendung“ von Michael Kofler, bei Addison-Wesley neu aufgelegt. Vier Jahre nach der siebten glänzt nun die achte Auflage in neuem Gewand. Mit Lesebändchen und in durchgehend zweifarbigem Druck präsentiert sich dem Leser ein detailreiches Panorama der gegenwärtigen Technik. Als Referenz-Distributionen verwendet der Autor Fedora 7, Ubuntu 7.04 (beide als DVDs im Buch), Opensuse 10.2, RHEL 5, Knoppix 5.2 und Debian 4.0, womit Letzteres endlich die ihm gebührende Beachtung erfährt.

Kofler gliedert den kaum zu bändigenden Stoff übersichtlich. Der Einstieg versetzt den Leser schon nach 120 Seiten in die Lage, mit dem System zu arbeiten. Gnome-Fans dürften erfreut sein: „Ihre“ Seitenzahl hat sich verdoppelt und zieht mit KDE gleich. Der zweite Teil bringt Neues bei den Desktop-Anwendungen. Die Ausführungen zu Web und Mail hat Kofler grundlegend überarbeitet, und das OpenOffice-Kapitel enthält jetzt die Datenbank-Komponente OOBase. Audio- und Video-Anwendungen bis hin zu Fernsehen mit DVB-T runden diesen Teil ab.

Tiefgründig wird es in den Kapiteln über Werkzeuge, Systemkonfiguration/Administration sowie Netz- und Serverkonfiguration. Kofler erklärt viele Sachverhalte distributionsübergreifend; wo es nötig ist, behandelt er Besonderheiten. Hervorzuheben ist das Kapitel über Dateiverwaltung, das umfassend auf Backup/Archivierung und ACLs/Extended Attributes eingeht, neue Werkzeuge wie Beagle und Tracker vorstellt und das *udev*-System des Kernel 2.6 erläutert. Neu sind Kapitel über Java, Mono und – auf vielfachen Leserwunsch – den Editor *vim*.

Fast 250 Seiten über Netz- und Server-Konfiguration hat der Autor ausdrücklich für Verwalter kleinerer Netze vorgesehen, sie sind jedoch anspruchsvolleren Lesern gleichermaßen zu empfehlen. Virtualisierungslösungen wie Wine, Xen und VMware ist ein eigener Buchteil gewidmet. Weitere Teile enthalten distributionsspezifische Informationen sowie eine thematische und alphabetische Kommandoreferenz, deren Umfang sich gegenüber früheren Auflagen nahezu verdoppelt hat. Gut gelungen ist der Index mit dreieinhalbtausend Fachbegriffen. Die Verweise führen wirklich an Stellen, an denen der Leser das Wesentliche erfährt, was bei Büchern dieser Art nicht immer der Fall ist.

Bei gleicher Höhe hat der Verlag das Buch etwas verbreitert. Die kleinere Schrift ist sogar besser lesbar als in den Vorauflagen. Die gut genutzte Marginalspalte hilft eine Überschrift-Ebene einzusparen und erhöht den Überblick. So darf man den neuen Kofler uneingeschränkt empfehlen.

DR. BERNHARD RÖHRIG



Ken Schwaber

Agiles Projektmanagement mit Scrum

Übersetzt von
Thomas Irlbeck
München 2007
Microsoft Press
164 Seiten
29,90 €
ISBN 978-3-86645-631-0

Scrum ist eine leicht zu erlernende Projektmanagementtechnik mit nur wenigen Regeln, die darauf setzen, dass sich die Beteiligten selbst verwalten, statt wie im klassischen Projektmanagement durch einen Projektleiter geführt zu werden.

Ken Schwaber, einer der Scrum-Erfinder, stellt anhand von Praxisbeispielen die agile Technik vor. Zunächst startet er mit einer knapp gehaltenen Einführung, die unerfahrene Leser besser nicht überspringen sollten. In den weiteren acht Kapiteln geht er auf die einzelnen Beteiligten ein (Scrum Master, Product Owner, Team). Dabei sind es nicht immer die Erfolgsgeschichten, die Schwaber präsentiert. Er zeigt gelegentlich explizit Fälle, in denen ein Scrum-Projekt nicht gut lief, weil bestimmte Voraussetzungen nicht stimmten oder Regeln von Scrum verletzt wurden.

Der Scrum Master ist für die Einhaltung der Regeln verantwortlich, er nimmt die Stelle eines sonstigen Projektleiters ein. Schwaber vergleicht ihn mit einem Schäferhund, der seine Herde (sie steht für das Team) vor den feindlichen Wölfen (Stackholdern, Projektinteressierten, die aber anders als die Stockholder nicht direkt beteiligt sind) verteidigen muss. Beispielsweise darf das Team während eines Sprints, dem 30 Tage währenden Entwicklungszyklus, nicht zusätzliche Aufgaben von außen aufgetragen bekommen, sondern es gilt der im Sprint Planning Meeting, dem dem Sprint vorgelagerten Planungstreffen, erstellte Product Backlog, der die in diesem Entwicklungsgang zu erstellenden (nicht) funktionalen Anforderungen enthält.

Wer Scrum als Vorgehensweise in die hauseigene Entwicklung einführen möchte, benötigt nicht sonderlich viele Werkzeuge, bei Schwaber Artefakte genannt. Die Korrelation zwischen dem verbleibenden Arbeitsaufwand und dem Projektfortschritt können Beteiligte einfach mit einer Tabellenkalkulation erstellen.

Das Buch enthält mehrere Anhänge, darunter Quellen zu Scrum für weiterführende Studien, einen Anhang zu Verträgen mit Festpreisen und garantierten Terminen sowie einen Anhang zum Capability Maturity Model, einem Prozessmodell zur Beurteilung der Qualität des Softwareprozesses in einer Organisation.

Wer die ausgetretenen Pfade des Projektmanagements und die Entwicklung nach dem Wasserfallmodell verlassen möchte, der findet in Scrum als inkrementeller Entwicklungsmethode eine recht brauchbare Alternative. Schwabers Buch lässt sich leicht lesen. Ob ein Studium des Bandes ausreicht, um Scrum im Unternehmen zu etablieren, sei hier dahingestellt. Wahrscheinlicher ist, dass man sich professionelle Hilfe zum Coachen ins Haus holen muss.

KARSTEN KISSER



Postfach 61 04 07, 30604 Hannover; Helstorfer Straße 7, 30625 Hannover

Redaktion
Telefon: 05 11/53 52-387, Fax: 05 11/53 52-361, E-Mail: post@ix.de
Abonnements: Telefon: 051 37/88 20 00, Fax: 051 37/88 17 12, E-Mail: abo@heise.de

Herausgeber: Christian Heise, Ansgar Heise

Redaktion: Chefredakteur: Jürgen Seeger (JS) -386

Stellv. Chefredakteur: Henning Behme (hb) -374

Ltd. Redakt.: Kersten Auel (ka) -367, Ralph Hülsenbusch (rh) -373, Bert Ungerer (un) -368

Jürgen Diercks (jd) -379, Christian Kirsch (ck) -590, Wolfgang Möhle (WM) -384, Susanne Nolte (sun) -689, André von Raison (avr) -377, Michael Riepe (mr) -787, Ute Roos (ur) -535

Redaktionsassistenz: Carmen Lehmann (cle) -387, Michael Mentzel (mm) -153

Korrespondent Köln/Düsseldorf/Ruhrgebiet:
Achim Born, Siebengebirgsallee 82, 50939 Köln,Telefon: 02 21/4 20 02 62,
E-Mail: ab@ix.de

Korrespondentin München:
Susanne Franke, Ansbacherstr. 2, 80796 München, Telefon: 089/28 80 74 80,
E-Mail: sf@ix.de

Ständige Mitarbeiter: Torsten Beyer, Detlef Borchers, Fred Hantelmann, Kai König, Michael Kuschke, Barbara Lange, Stefan Mintert, Holger Schwichtenberg, Susanne Schwonbeck, Christian Segor, Diane Sieger, Axel Wilzopolski, Nikolai Zotow

DTP-Produktion: Enrico Eisert, Wiebke Preuß, Matthias Timm, Hinstorff Verlag, Rostock

Korrektorat/Chefin vom Dienst: Anja Fischer

Fotografie: Martin Klauss Fotografie, Despetal/Barfelde

Titelidee: ***iX;*** Titel- und Aufmachergestaltung: Dietmar Jokisch

Verlag und Anzeigenverwaltung:
Heise Zeitschriften Verlag GmbH & Co. KG, Postfach 61 04 07, 30604 Hannover;
Helstorfer Straße 7, 30625 Hannover; Telefon: 05 11/53 52-0, Fax: 05 11/53 52-129

Geschäftsführer: Ansgar Heise, Steven P. Steinkraus, Dr. Alfons Schräder

Mitglied der Geschäftsleitung: Beate Gerold

Verlagsleiter: Dr. Alfons Schräder

Anzeigenleitung: Michael Hanke -167, E-Mail: michael.hanke@heise.de

Assistenz: Christine Richter -534, E-Mail: christine.richter@heise.de

Anzeigendisposition: Christine Richter -534, E-Mail: christine.richter@heise.de

Anzeigenverkauf: PLZ-Gebiete 0–3, Ausland:
Oliver Kühn -395, E-Mail: oliver.kuehn@heise.de,
PLZ-Gebiete 8–9: Ralf Räuber -218, E-Mail: ralf.raeuber@heise.de
Sonderprojekte: Isabelle Paeseler -205, E-Mail: isabelle.paeseler@heise.de

Anzeigen-Inlandsvertretung: PLZ-Gebiete 4–7:
Karl-Heinz Kremer GmbH, Sonnenstraße 2, D-66957 Hilst,
Telefon: 063 35/92 17-0, Fax: 063 35/92 17-22, E-Mail: karlheinz.kremer@heise.de

Anzeigen-Auslandsvertretung:
Großbritannien, Irland: Oliver Smith & Partners Ltd. Colin Smith, 18 Abbeville Mews, 88 Clapham Park Road, London SW4 7BX, UK, Telefon: (00 44) 20/79 78-14 40, Fax: (00 44) 20/79 78-15 50, E-Mail: colin@osp-uk.com

Anzeigenpreise: Es gilt die Anzeigenpreisliste Nr. 20 vom 1. Januar 2008.

Leiter Vertrieb und Marketing: Mark A. Cano (-299); Abo-Service, Telefon: +49 (0) 711/7252-292

Werbeleitung: Julia Conrades (-156)

Teamleitung Herstellung: Bianca Nagel (-456)

Druck: Dierichs Druck + Media GmbH & Co. KG, Kassel

Sonderdruck-Service: Ruth Utesch (-359, Fax: -360)

Verantwortlich: Textteil: Jürgen Seeger; Anzeigenteil: Michael Hanke

***iX* erscheint monatlich**

Einzelpreis € 5,50, Österreich € 6,20, Schweiz CHF 10,70, Benelux € 6,70, Italien € 6,70

Das Abonnement für 12 Ausgaben kostet: Inland € 56,–, Ausland (außer Schweiz) € 63,–; Studentenabonnement: Inland € 42,00, Ausland (außer Schweiz) € 47,00 nur gegen Vorlage der Studienbescheinigung (inkl. Versandkosten Inland € 8,30, Ausland € 13,30), Luftpost auf Anfrage.

iX-Abo+ (inkl. jährlicher Archiv-CD-ROM) jeweils zzgl. € 8,–

Für GI-, VDI-KfIT-, GUUG-, IUG-, LUG-, AUGE- und Mac-e.V.-Mitglieder gilt der Preis des Studentenabonnements (gegen Mitgliedsausweis).

Kundenkonto in Österreich:
Dresdner Bank AG, BLZ 19675, Kto.-Nr. 2001-226-00 EUR, SWIFT: DRES AT WX

Kundenkonto in der Schweiz: UBS AG, Zürich, Kto.-Nr. 206 P0-465.060.0

Abo-Service:
Heise Zeitschriften Verlag, Kundenservice, Postfach 810520, 70522 Stuttgart,
Telefon: +49 (0) 711/72 52-292, Fax: +49 (0) 711/72 52-392, E-Mail: abo@heise.de

Für Abonnenten in der Schweiz Bestellung über:
Thali AG, Aboservice, Industriestr. 14, CH-6285 Hitzkirch,
Telefon: 041/919 66 11, Fax: 041/919 66 77, E-Mail: abo@thali.ch, Internet: www.thali.ch (Jahresabonnement: CHF 111,–; Studentenabonnement: CHF 83,25)

Das Abonnement ohne Archiv-CD-ROM ist jederzeit mit Wirkung zur jeweils übernächsten Ausgabe kündbar. Das *iX-Abo+* (incl. jährlicher Archiv-CD-ROM) gilt zunächst für ein Jahr und ist danach zur jeweils übernächsten Ausgabe kündbar.

Vertrieb Einzelverkauf (auch für Österreich, Luxemburg und Schweiz): MZV Moderner Zeitschriften Vertrieb GmbH & Co. KG, Breslauer Str. 5, 85386 Eching, Telefon: 089/31906-0, Fax: 089/31906-113, E-Mail: mzv@mzv.de, Internet:: www.mzv.de

ISSN 0935-9680





Apples Leopard Server

Wenn von Apples Betriebssystem Mac OS X die Rede ist, dürften viele an das schicke MacBook, den Mac mini oder den iMac denken. Deshalb drehen sich die zahlreichen Diskussionen über Apples neues Mac OS X 10.5 „Leopard“ um den Desktop. Dabei hat die Server-Variante Neuigkeiten zu bieten, die in der Desktop-Version fehlen. Auf einem iMac-Server „Xserve“ konnte Mac OS X 10.5 seine Stärken ausspielen und zeigen, was die Wandlung vom Tiger zum Leoparden mit sich bringt.

Thin Clients und mehr

Die Debatten um stetig steigende Strompreise und den Klimawandel haben längst die IT-Branche erreicht. Dabei verursachen PCs und Arbeitsplatzrechner den Löwenanteil der durch IT verursachten Stromkosten und CO_2-Emissionen. Vor allem Anbieter von Thin Clients und Mini-PCs bekommen dadurch Oberwasser. Zugleich wächst die Anzahl der ultraschlanken Clients und der Strom sparenden Thin-Client-Alternativen – eine Marktübersicht.

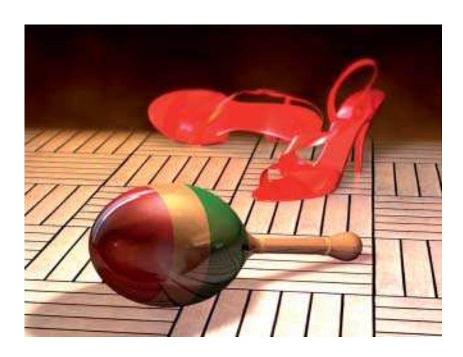
Server-Offensive

Letztes Jahr lief Microsofts Client-Offensive mit Vista, Office und den damit verbundenen Exchange- und Sharepoint-Servern. Im Februar 2008 will das Imperium mit diversen Varianten des Windows Server, dem IIS7, der MS-SQL-Datenbank, einem stark aufgebohrten .Net Framework sowie einer Neuauflage der eigenen IDE Visual Studio serverseitig nachziehen. *iX* stellt die neuen Produkte unter dem Aspekt der Interoperabilität vor.

Heft 3/2008 erscheint 21. Februar 2008

Per 2D-Barcode ins Internet

Als Briefmarkenersatz dürfte sie jeder schon gesehen haben: 2D-Barcodes, die deutlich mehr Informationen transportieren können als ihre eindimensionalen Pendants – zum Beispiel Webadressen. Wenn noch das internetfähige Foto-Handy als Barcode-Leser zum Einsatz kommt, steht der direkten Verknüpfung von realer Welt und World Wide Web nichts mehr im Weg.

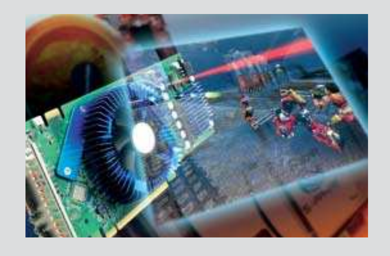


Musische Anwandlungen

Die IT-Welt weiß, dass Samba mehr ist als Musik und Tanz. Geht es um die Konfiguration der freien SMB/CIFS-Implementierung, nimmt das Know-how schnell ab – je nach Komplexität der zu bewältigenden Aufgabe. Ein dreiteiliges Tutorial führt in die Tiefen der fast 150 Samba-Konfigurationsparameter ein und gibt Tipps zum Betrieb der zum Paket gehörenden Programme. Start mit dem ersten Teil im kommenden Heft.

Das bringen





Grafikkarten: Viel 3D-Leistung fürs Geld

Projektoren: Kinospaß mit Full-HD

Medienserver: Die private Sammlung weltweit im Zugriff

DVD-Brenner: Sichere Daten trotz Spottpreis?

Heft 3/08 ab 21. Januar am Kiosk





Ökologie: Neue Gesetze treiben Gebäudetechnik voran

Sozial suchen: Wie Suchmaschinen und soziale Netze verschmelzen

Doppelt fährt besser: Die besten Getriebekonzepte für Hybridautos

Heft 2/08 ab 24. Januar am Kiosk

TELEPOLIS
MAGAZIN DER NETZKULTUR



Stefan Höltgen: Ein Spiel und ein Film erzählen die Geschichte der USA

Goedart Palm: Virtueller Blüthenstaub – Von der Romantik und dem deutschen Wesen

www.heise.de/tp/